

QUANTUM BILINEAR OPTIMIZATION

MARIO BERTA, OMAR FAWZI, AND VOLKHER B. SCHOLZ

ABSTRACT. We study optimization programs given by a bilinear form over noncommutative variables subject to linear inequalities. Problems of this form include the entangled value of two-prover games, entanglement assisted coding for classical channels and quantum-proof randomness extractors. We introduce an asymptotically converging hierarchy of efficiently computable semidefinite programming (SDP) relaxations for this quantum optimization. This allows us to give upper bounds on the quantum advantage for all of these problems. Compared to previous work of Pironio, Navascués and Acín, our hierarchy has additional constraints. By means of examples, we illustrate the importance of these new constraints both in practice and for analytical properties. Moreover, this allows us to give a hierarchy of SDP outer approximations for the completely positive semidefinite cone introduced by Laurent and Piovesan.

1. INTRODUCTION

1.1. Setting. A major goal in quantum information theory is to understand the advantage over classical protocols that can be achieved by allowing quantum protocols. For a given information processing task, identifying the optimal success rate for this task can be seen as an optimization over the set of valid protocols. The quantum advantage is then defined as the increase in the optimal value by allowing a larger set of protocols that make use of quantum theory. A family of tasks for which such an advantage is very well-studied is the family of games between multiple parties that are not allowed to communicate. As was first demonstrated by Bell [3, 15], there exist games for which entanglement between the players can increase the success probability beyond the ultimate limit of classical protocols. The fundamental limit for classical protocols is called a Bell inequality and its violation indicates an important feature of quantum theory called nonlocality. The topic of nonlocality has been a very active topic in quantum information theory and in the foundations of quantum mechanics; see [11] for a review. A quantum advantage can also be studied in many other settings including communication complexity [12], communication over a classical channel [18, 43] or randomness extractors [44]. One objective of this paper is to formulate many of these problems in a unified language as bilinear optimization programs.

To make the discussion more concrete, we consider a specific example. Let $W_{X \rightarrow Y}$ be a noisy channel mapping system X to system Y . Assuming X and Y are discrete systems, we can describe the channel by the transition probabilities $W_{X \rightarrow Y}(y|x)$ from x to y for all $(x, y) \in X \times Y$. The goal is to send k bits of information using this channel while minimizing the error probability for the decoding. A valid protocol in this setting is given by an encoding function $e : [2^k] \rightarrow X$ and a decoding function $d : Y \rightarrow [2^k]$. To take into account the possibility of a randomized functions, we describe the encoder by a probability distribution $\{e(x|i)\}_x$ on X for every possible input $i \in [2^k]$, and similarly the decoder by a distribution $\{d(i|y)\}_i$ on $[2^k]$ for every $y \in Y$. Given an encoder and a decoder, the average success probability of our protocol can be expressed as $\frac{1}{2^k} \sum_{x,y,i} d(i|y) W_{X \rightarrow Y}(y|x) e(x|i)$. In summary, optimizing the success probability of information transmission is captured by the following bilinear program

$$\begin{aligned}
 (1) \quad & \underset{(e,d)}{\text{maximize}} && \frac{1}{2^k} \sum_{x,y,i} W_{X \rightarrow Y}(y|x) d(i|y) e(x|i) \\
 & \text{subject to} && \sum_x e(x|i) = 1 \quad \forall i \in [2^k] \\
 & && \sum_i d(i|y) = 1 \quad \forall y \in Y \\
 & && 0 \leq e(x|i) \leq 1 \quad \forall (x, i) \in X \times [2^k] \\
 & && 0 \leq d(i|y) \leq 1 \quad \forall (i, y) \in [2^k] \times Y.
 \end{aligned}$$

Observe that allowing the encoder and the decoder to access (unlimited) shared randomness does not change the optimal value of this program. A fundamental question is to study the effect of shared entanglement for information transmission. Shared entanglement by itself is useless for information transmission, but it is known that it can offer important advantages for information transmission over a quantum channel [5, 7, 6], and even for a classical channel [18, 43]. The latter is the setting we consider here. A quantum protocol is described by a Hilbert space \mathcal{H} , a state $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}$ shared between the encoder and the decoder, and positive operator-valued measures on \mathcal{H} for the encoder $\{E(x|i)\}_x$ for each $i \in [2^k]$ and for the decoder $\{D(i|y)\}_i$ for each $y \in Y$. In the quantum setting, optimizing the success probability for transmitting k bits is given by

$$\begin{aligned}
 (2) \quad & \underset{(\mathcal{H}, \psi, E, D)}{\text{maximize}} && \frac{1}{2^k} \sum_{x, y, i} W_{X \rightarrow Y}(y|x) \langle \psi | E(x|i) \otimes D(i|y) | \psi \rangle \\
 & \text{subject to} && \sum_x E(x|i) = \text{id}_{\mathcal{H}} \quad \forall i \in [2^k] \\
 & && \sum_i D(i|y) = \text{id}_{\mathcal{H}} \quad \forall y \in Y \\
 & && 0 \leq E(x|i) \leq \text{id}_{\mathcal{H}} \quad \forall (x, i) \in X \times [2^k] \\
 & && 0 \leq D(i|y) \leq \text{id}_{\mathcal{H}} \quad \forall (i, y) \in [2^k] \times Y.
 \end{aligned}$$

As we can always take $\mathcal{H} = \mathbb{C}$, any feasible solution for (1) is also a feasible solution for (2).

Allowing for quantum protocols also leads to the definition of quantum graph parameters [14, 45, 34, 13]. For example, the stability number of a graph G can be viewed in terms of the success probability of a two-prover game depending on G , or in terms of the success probability for information transmission over a noisy channel defined by G . Allowing quantum protocols in these tasks naturally leads to the definition of quantum stability numbers of a graph. To study such quantum graph parameters, Laurent and Piovesan [34] recently introduced a noncommutative analog of the completely positive cone \mathcal{CP} called the completely positive semidefinite cone \mathcal{CS}_+ . For the aforementioned problems, the set of quantum strategies can then be described using \mathcal{CS}_+ , and the quantum advantage is witnessed by the fact \mathcal{CS}_+ is larger than \mathcal{CP} .

Having phrased the setup, let us now give a short overview of our findings.

1.2. Results. We start by phrasing problems like the ones stated above as optimization programs. More precisely, we study the class of tasks that can be described by optimizing a bilinear function subject to linear inequalities. The optimization over classical protocols corresponds to a program similar to (1) with commutative (scalar) variables, whereas the optimization over quantum protocols corresponds to allowing the variables to be matrix-valued as in (2). As it appears from the expression, optimization over quantum protocol seems quite complicated. In fact, as there is no bound on the dimension of the Hilbert space, it is not known whether the optimal value is even computable. In the context of games, Navascués, Pironio and Acín (NPA) [35] introduced a family of semidefinite programming (SDP) relaxations that give efficiently computable upper bounds on quantum bilinear programs. This hierarchy was shown to asymptotically converge to the optimal quantum protocol [36, 41, 19]. These hierarchies can be seen as noncommutative versions of the sum-of-squares hierarchies introduced by Lasserre and Parrilo [33, 40].

Our first contribution is the observation that many information processing tasks can be formulated in this way. We believe that phrasing these seemingly different problems in a unified language will help in our understanding of each one of these problems. Moreover, we think that tools developed in the context of optimization should be valuable in characterizing the power and limitations of quantum protocols. Our second contribution is to give a new hierarchy of SDPs that gives upper bounds on quantum bilinear programs. Compared to the previous contributions [35, 36, 41, 19], our hierarchy has some additional constraints which we illustrate to be useful in several settings. For example, the first level of our hierarchy has the nice property of being naturally bounded by the maximal value of the general problem, i.e., it is bounded by one for the case of channel coding discussed above. In addition, by means of a specific example, we show that our SDPs can give better bounds in practice. The new constraints are also necessary to examine the relationship of our approach to the one by Laurent and Piovesan [34]: we show that they lead to a natural hierarchy of SDP outer approximations for the completely positive semidefinite cone \mathcal{CS}_+ .

1.3. Organization of the Paper. In Section 2, we introduce the general setup of quantum bilinear optimization and present our new hierarchy of SDPs. We keep the main text elementary and only prove that our SDPs give upper bounds on the quantum programs when the Hilbert space is finite dimensional (the infinite dimensional case as well as the convergence of the hierarchy are deferred to appendices). In Section 3, we describe applications to two-prover games, channel coding, randomness extractors as well as to the optimization over the completely positive semidefinite cone.

2. BILINEAR OPTIMIZATION

2.1. Setup. As motivated in (1) we would like to start from the following type of (classical) bilinear optimization program with real variables z_α for $\alpha \in [N] := \{1, \dots, N\}$ and y_β for $\beta \in [M] := \{1, \dots, M\}$,¹

$$(3) \quad \begin{aligned} p[A, \mathcal{G}, \mathcal{K}] &:= \underset{(z_\alpha, y_\beta)}{\text{maximize}} \quad \sum_{\alpha, \beta} A_{\alpha, \beta} z_\alpha y_\beta \\ &\text{subject to} \quad g(z_1, \dots, z_N) \geq 0 \quad \forall g \in \mathcal{G} \\ &\quad k(y_1, \dots, y_M) \geq 0 \quad \forall k \in \mathcal{K}. \end{aligned}$$

with sets of linear constraints $\mathcal{G} := \{g(z_1, \dots, z_N)\}$ and $\mathcal{K} := \{k(y_1, \dots, y_M)\}$, where

$$(4) \quad g(z_1, \dots, z_N) := g^0 + \sum_{\alpha \in [N]} g^\alpha z_\alpha \quad \text{and} \quad k(y_1, \dots, y_M) := k^0 + \sum_{\beta \in [M]} k^\beta y_\beta.$$

For convenience we also define the complete set of constraints

$$(5) \quad \mathcal{F} := \mathcal{G} \cup \mathcal{K} \cup \{f_z\}$$

including the trivial constraint $f_z := 1$ and call

$$(6) \quad p[A, \mathcal{F}] := p[A, \mathcal{G}, \mathcal{K}]$$

the classical value of (3).

In analogy to (2) the corresponding quantum bilinear optimization program of (3) is then as follows. Let \mathcal{H} be a Hilbert space (of arbitrary dimension), $\psi \in \mathcal{H}$ with $\|\psi\| = 1$, and let E_α, D_β be Hermitian operators in the algebra $\mathcal{B}(\mathcal{H})$ of bounded linear operators on \mathcal{H} . By substituting the variables z_α in the linear constraints with operators E_α (and similarly for y_β with D_β) we set

$$(7) \quad \begin{aligned} p^*[A, \mathcal{G}, \mathcal{K}] &:= \underset{(\mathcal{H}, \psi, E_\alpha, D_\beta)}{\text{maximize}} \quad \sum_{\alpha, \beta} A_{\alpha, \beta} \langle \psi | E_\alpha D_\beta | \psi \rangle \\ &\text{subject to} \quad [E_\alpha, D_\beta] = 0 \quad \forall (\alpha, \beta) \in [N] \times [M] \\ &\quad g(E_1, \dots, E_N) \geq 0 \quad \forall g \in \mathcal{G} \\ &\quad k(D_1, \dots, D_M) \geq 0 \quad \forall k \in \mathcal{K}, \end{aligned}$$

where $[E_\alpha, D_\beta] := E_\alpha D_\beta - D_\beta E_\alpha$ denotes the commutator, and $g(E_1, \dots, E_N) \geq 0$ means that the operator $g(E_1, \dots, E_N)$ is positive semidefinite (and similarly for $k(D_1, \dots, D_M) \geq 0$). In the following we call

$$(8) \quad p^*[A, \mathcal{F}] := p^*[A, \mathcal{G}, \mathcal{K}]$$

the quantum value of (7), with the total set of constraints \mathcal{F} as in (5). Clearly the quantum value is never smaller than the classical value,

$$(9) \quad p[A, \mathcal{F}] \leq p^*[A, \mathcal{F}].$$

Note that compared to the entanglement assisted channel coding example (2) we do not assume that the Hilbert space \mathcal{H} has tensor product form with E_α acting on the first factor and D_β acting on the second factor, but only that E_α and D_β commute. This takes into account the most general formulation of quantum mechanics [26] (see also [10] for a quantum information theory reference). However, for every feasible solution of (7) corresponding to a finite dimensional Hilbert space, we can assume that the Hilbert space has a tensor product structure $\mathcal{H} \otimes \mathcal{H}$ with operators $E_\alpha \otimes \mathbb{1}$ and $\mathbb{1} \otimes D_\beta$ (instead of just $[E_\alpha, D_\beta] = 0$ on a single space \mathcal{H}); see e.g., [48, Chapter 5] or for a self-contained quantum information theory reference [46]. Moreover, for the general infinite-dimensional

¹Here and henceforth we write maximize for taking the supremum (in particular the maximum might not be attained).

case the optimal value of (2) is certainly upper bounded by the optimal value of the corresponding program (7).

Remark 2.1. *Provided Connes' embedding conjecture has a positive answer [17, 38], we can restrict the optimization in (7) to finite dimensional Hilbert spaces (and thus of tensor product form). This was proved for the special case of bipartite games in [28, 22]. For a proof sketch for the general case see Appendix B.*

Our ultimate goal is to understand the gap between the classical value $p[A, \mathcal{F}]$ and the quantum value $p^*[A, \mathcal{F}]$ for operational examples of interest. For the problems that we study in this paper $p[A, \mathcal{F}]$ is typically understood but estimating $p^*[A, \mathcal{F}]$ is the challenge. Lower bounds on $p^*[A, \mathcal{F}]$ can then be found by any feasible solution of (7) but upper bounds are harder to find (basically because the optimization in (7) is over Hilbert spaces of unbounded dimension). Building on the works of Navascués, Pironio and Acín [35, 36] and Doherty, Liang, Toner and Wehner [19] in the context of games, Pironio, Navascués and Acín [41] gave asymptotically converging hierarchies of SDP relaxations for general quantum polynomial optimization (see [23] for an operator algebra point of view on this hierarchy). We briefly sketch their results when applied to our more specific setting of quantum bilinear optimization as in (7).

2.2. NPA Hierarchy. We first introduce some notation. Let Σ_∞ denote the free complex $*$ -algebra generated by the $N + M$ symbols

$$(10) \quad z_1, \dots, z_N, y_1, \dots, y_M.$$

In other words, these are the noncommutative polynomials in the variables z, y . The monomials of Σ_∞ are also called words and can be indexed by a tuple $u = (u_1, \dots, u_\ell)$ with $u_i \in \{1, \dots, N + M\}$. For example, the monomial x_u indexed by $u = (1, 3, 3, N + 2)$ is defined as $x_u = z_1 z_3^2 y_2$. The degree of a monomial x_u , which is also called the length of the word is denoted $\ell(u)$. The unit monomial x_\emptyset is called the empty word indexed by the empty tuple \emptyset , and has length zero. Words $u, v \in \Sigma_\infty$ are concatenated as

$$(11) \quad u \circ v := (u_1, \dots, u_{\ell(u)}, v_1, \dots, v_{\ell(v)}).$$

The algebra Σ_∞ also carries a natural involution $*$: $\Sigma_\infty \rightarrow \Sigma_\infty$ reversing the order of words $(u \circ v)^* := v \circ u$ and being the complex conjugation for complex scalars. For a fixed integer $n \in \mathbb{N}$, the set of words (monomials) of length up to n , $\ell(w) \leq n$, spans a vector space Σ_n of dimension

$$(12) \quad d(n) := \frac{(N + M)^{n+1} - 1}{N + M - 1}.$$

Now for every feasible solution $(\mathcal{H}, \psi, E_\alpha, D_\beta)$ of (7), NPA define the linear form

$$(13) \quad \tilde{\omega} : \Sigma_\infty \rightarrow \mathbb{C} \quad \text{with} \quad \tilde{\omega}(u) := \langle \psi | X_u | \psi \rangle,$$

where X_u stands for the explicit representation of the word x_u in terms of the operators E_α and D_β for the symbols z_α and y_β , respectively. Then NPA look at the (infinite-dimensional) matrix

$$(14) \quad \tilde{\Omega} := \sum_{u, v} \tilde{\Omega}_{u, v} |u\rangle \langle v| \quad \text{with entries} \quad \tilde{\Omega}_{u, v} := \langle \psi | X_u^* X_v | \psi \rangle.$$

This matrix is positive semidefinite since it is the Gram matrix of the vectors $X_v | \psi \rangle$. Moreover, the linear constraints $f \in \mathcal{F}$ generate (infinite-dimensional) matrices

$$(15) \quad \tilde{\Omega}[f] := \sum_{i=0}^N f^i \sum_{u, v} \tilde{\Omega}_{u, (i) \circ v} |u\rangle \langle v|$$

that are positive semidefinite as well (where the tuple (i) indexes words of length one: the i -th symbol). For the commutativity constraints between E_α and D_β , this can be simply captured by identifying words $u \sim v$ if v can be obtained from u by using commutation between z_α and y_β . For example, $z_1 y_3 z_2^2 \sim z_1 z_2^2 y_3$. Restricting in (14) and (15) to constraints that only involve words up to length n

defines the n -th level of the NPA hierarchy. In more detail, for any $n \geq 1$

$$\begin{aligned}
 \text{sdp}_n[A, \mathcal{F}] &:= \underset{\tilde{\Omega}^n}{\text{maximize}} && \sum_{\alpha, \beta} A_{\alpha, \beta} \tilde{\Omega}_{(\alpha), (\beta)}^n \\
 &\text{subject to} && \tilde{\Omega}^n \in \text{Pos}(d(n)) \\
 &&& \tilde{\Omega}_{\emptyset, \emptyset}^n = 1 \\
 &&& \tilde{\Omega}_{u, v^* \circ w}^n = \tilde{\Omega}_{v \circ u, w}^n \quad \forall u, v, w \in \Sigma_n : u \circ v \in \Sigma_n, v \circ w \in \Sigma_n \\
 &&& \tilde{\Omega}_{u, v}^n = \tilde{\Omega}_{u', v'}^n \quad \forall u, u', v, v' \in \Sigma_n : u \sim u', v \sim v' \\
 &&& \tilde{\Omega}^n[f] := \sum_{i=0}^{N+M} f^i \sum_{u, v \in \Sigma_{n-1}} \tilde{\Omega}_{u, (i) \circ v}^n |u\rangle \langle v| \in \text{Pos}(d(n-1)) \quad \forall f \in \mathcal{F},
 \end{aligned} \tag{16}$$

where $\text{Pos}(d(n))$ denotes the set of positive semidefinite matrices of size $d(n)$ as in (12), and we have the total set of constraints \mathcal{F} as in (5). In the literature the matrices $\tilde{\Omega}^n$ are called moment matrices while the matrices $\tilde{\Omega}^n[f]$ are called localizing matrices. Clearly the levels of the NPA hierarchy are monotonically decreasing in the sense that for any $n \in \mathbb{N}$,

$$\text{sdp}_n[A, \mathcal{F}] \geq \text{sdp}_{n+1}[A, \mathcal{F}], \tag{17}$$

and by the preceding discussion we also have

$$p^*[A, \mathcal{F}] \leq \text{sdp}_n[A, \mathcal{F}]. \tag{18}$$

Moreover, if the constraints are such that there exists a real constant C with

$$\forall \alpha \in [N] : C\mathbb{1} \geq E_\alpha \geq -C\mathbb{1} \quad \text{and} \quad \forall \beta \in [M] : C\mathbb{1} \geq D_\beta \geq -C\mathbb{1}, \tag{19}$$

then the NPA hierarchy asymptotically converges to the optimal value [19, 36, 41],

$$p^*[A, \mathcal{F}] = \lim_{n \rightarrow \infty} \text{sdp}_n[A, \mathcal{F}]. \tag{20}$$

The condition (19) is called Archimedian and is typically fulfilled for all examples of interest. In the following we will always assume the set of constraints \mathcal{F} includes the Archimedian constraints (19).

The first few levels of the NPA hierarchy have been used intensively in order to understand the separation between the classical and the quantum value of two-prover games, see e.g., [39]. In the following we propose an alternative SDP hierarchy. This hierarchy is not only useful for studying two-prover games but also for other problems like (entanglement assisted) one-shot channel coding, (quantum-proof) randomness extractors, and for optimizations over the completely positive semidefinite cone.

2.3. New Hierarchy. We use a way different from (15) for generating constraints. Instead of defining the NPA linear form $\tilde{\omega}$ as in (13) we define a bilinear form $\omega : \Sigma_\infty \times \Sigma_\infty \rightarrow \mathbb{C}$ that we now describe for the case of finite-dimensional Hilbert spaces. The general case can be found in Appendix A. Now as stated above, for finite dimensions we can assume that the noncommutative optimization in (7) is over tensor product Hilbert spaces $\mathcal{H} \otimes \mathcal{H}$ with operators $E_\alpha \otimes \mathbb{1}$ and $\mathbb{1} \otimes D_\beta$ (instead of just $[E_\alpha, D_\beta] = 0$ on a single space \mathcal{H}). We start with any feasible solution $(\mathcal{H} \otimes \mathcal{H}, \psi, E_\alpha \otimes \mathbb{1}, \mathbb{1} \otimes D_\beta)$ where again the operators E_α are explicit representations of the symbols z_α and the operators D_β are explicit representations of the symbols y_β . Taking the partial trace over one space \mathcal{H} we denote

$$\sigma := \text{Tr}_{\mathcal{H}} [|\psi\rangle\langle\psi|] \quad \text{and write} \quad |\psi\rangle = \left(U \otimes \sigma^{1/2} \right) |\Phi\rangle, \tag{21}$$

where $|\Phi\rangle := \sum_i |i\rangle|i\rangle$ for some orthonormal basis $\{|i\rangle\}$ of \mathcal{H} and a unitary U . The objective function of the quantum bilinear optimization program (7) can then be rewritten as

$$\sum_{\alpha, \beta} A_{\alpha, \beta} \langle \psi | U E_\alpha U^\dagger \otimes D_\beta | \psi \rangle = \sum_{\alpha, \beta} A_{\alpha, \beta} \langle \Phi | U E_\alpha U^\dagger \otimes (\sigma^{1/2} D_\beta \sigma^{1/2}) | \Phi \rangle \tag{22}$$

$$= \sum_{\alpha, \beta} A_{\alpha, \beta} \text{Tr} \left[\bar{U} E_\alpha^T U^T \sigma^{1/2} D_\beta \sigma^{1/2} \right], \tag{23}$$

where E^T denotes the transpose of the operator E and \bar{U} is the complex conjugate of U in the basis $\{|i\rangle\}$ of \mathcal{H} . We note that the transpose as well as the conjugation by unitary operators preserve our

constraints, and hence may be just absorbed in the operators E_α , as we maximize over them. Hence, we get the following alternative form of (7),

$$(24) \quad \begin{aligned} p^*[A, \mathcal{G}, \mathcal{K}] = & \underset{(\sigma, E_\alpha, D_\beta)}{\text{maximize}} && \sum_{\alpha, \beta} A_{\alpha, \beta} \text{Tr} \left[E_\alpha \sigma^{1/2} D_\beta \sigma^{1/2} \right] \\ & \text{subject to} && \sigma \geq 0, \text{Tr}[\sigma] = 1 \\ & && g(E_1, \dots, E_N) \geq 0 \quad \forall g \in \mathcal{G} \\ & && k(D_1, \dots, D_M) \geq 0 \quad \forall k \in \mathcal{K}. \end{aligned}$$

Now we define the bilinear form

$$(25) \quad \omega : \Sigma_\infty \times \Sigma_\infty \rightarrow \mathbb{C} \quad \text{with} \quad \omega(u, v) := \text{Tr} \left[X_u \sigma^{1/2} X_v \sigma^{1/2} \right].$$

Similarly as for NPA we look at the (infinite-dimensional) matrix

$$(26) \quad \Omega := \sum_{u, v} \Omega_{u, v} |u\rangle\langle v| \quad \text{with entries} \quad \Omega_{u, v} := \omega(u^*, v) = \text{Tr} \left[X_{u^*} \sigma^{1/2} X_v \sigma^{1/2} \right] = \langle \psi | X_{u^*}^T \otimes X_v | \psi \rangle$$

and find that it is positive semidefinite. However, the bilinear form (25) gives us even more structure. Namely we can say that the reordered (infinite-dimensional) matrix

$$(27) \quad \Omega[1, 1] := \sum_{s, t, u, v} \Omega_{s^* \circ t, u^* \circ v} |s\rangle\langle t| \otimes |u\rangle\langle v|$$

is positive semidefinite as well. To see this, take a vector $|\phi\rangle = \sum_{s, u} c_{s, u} |s\rangle |u\rangle$. Then, we have

$$(28) \quad \begin{aligned} \langle \phi | \Omega[1, 1] | \phi \rangle &= \sum_{s, t, u, v} \bar{c}_{s, u} c_{t, v} \text{Tr} \left[X_{t^*} X_s \sigma^{1/2} X_{u^*} X_v \sigma^{1/2} \right] \\ &= \sum_{s, t, u, v} \bar{c}_{s, u} c_{t, v} \text{Tr} \left[X_s \sigma^{1/2} X_{u^*} X_v \sigma^{1/2} X_{t^*} \right] \end{aligned}$$

$$(29) \quad = \text{Tr} \left[\left(\sum_{s, u} \bar{c}_{s, u} X_s \sigma^{1/2} X_{u^*} \right) \left(\sum_{t, v} c_{t, v} X_v \sigma^{1/2} X_{t^*} \right) \right]$$

$$(30) \quad = \text{Tr} \left[\left(\sum_{s, u} c_{s, u} X_u \sigma^{1/2} X_{s^*} \right)^* \left(\sum_{s, u} c_{s, u} X_u \sigma^{1/2} X_{s^*} \right) \right] \geq 0.$$

More generally, any pair of linear constraints $f, \bar{f} \in \mathcal{F}$ from (5) generate (infinite-dimensional) matrices

$$(31) \quad \Omega[f, \bar{f}] := \sum_{i, j=0}^{N+M} f^i \bar{f}^j \sum_{r, s, u, v} \Omega_{r^* \circ (i) \circ s, u^* \circ (j) \circ v} |r\rangle\langle s| \otimes |u\rangle\langle v|$$

that are positive semidefinite. Now restricting in (26) and (31) to constraints that only involve words up to length n defines the n -th level of our new hierarchy. That is, for n odd we define

$$(32) \quad \begin{aligned} \text{sdp}_n[A, \mathcal{F}] := & \underset{\Omega^n}{\text{maximize}} && \sum_{\alpha, \beta} A_{\alpha, \beta} \Omega_{(\alpha), (\beta)}^n \\ & \text{subject to} && \Omega^n \in \text{Pos}(d(n)) \\ & && \Omega_{\emptyset, \emptyset}^n = 1 \\ & && \Omega^n[f, \bar{f}] := \sum_{i, j=0}^{N+M} f^i \bar{f}^j \sum_{r, s, u, v \in \Sigma_{(n-1)/2}} \Omega_{r^* \circ (i) \circ s, u^* \circ (j) \circ v}^n |r\rangle\langle s| \otimes |u\rangle\langle v| \\ & && \in \text{Pos}(d^2(n-1)) \quad \forall f, \bar{f} \in \mathcal{F}. \end{aligned}$$

For $n \geq 2$ even, we replace the last constraint in (32) with the following constraints where $n' := (n-2)/2$:

$$\begin{aligned}
 \Omega^n[1, 1] &:= \sum_{\substack{r, s \in \Sigma_{n/2} \\ u, v \in \Sigma_{n/2}}} \Omega_{r^* \circ s, u^* \circ v}^n |r\rangle\langle s| \otimes |u\rangle\langle v| \in \text{Pos}\left(d(n/2)d(n/2)\right) \\
 \Omega^n[f] &:= \sum_{i=0}^{N+M} f^i \sum_{\substack{r, s \in \Sigma_{n'} \\ u, v \in \Sigma_{n/2}}} \Omega_{r^* \circ (i) \circ s, u^* \circ v}^n |r\rangle\langle s| \otimes |u\rangle\langle v| \in \text{Pos}\left(d(n')d(n/2)\right) \quad \forall f \in \mathcal{F} \\
 \Omega^n[f, \bar{f}] &:= \sum_{i=0}^{N+M} f^i \bar{f}^j \sum_{\substack{r, s \in \Sigma_{n'} \\ u, v \in \Sigma_{n/2}}} \Omega_{r^* \circ (i) \circ s, u^* \circ (j) \circ v}^n |r\rangle\langle s| \otimes |u\rangle\langle v| \in \text{Pos}\left(d(n')d(n')\right) \quad \forall f, \bar{f} \in \mathcal{F}.
 \end{aligned}
 \tag{33}$$

In accordance with the literature we call the matrices Ω^n moment matrices and the matrices $\Omega^n[f, \bar{f}]$, $\Omega^n[f]$ localizing matrices. Clearly the levels of this new hierarchy are monotonically decreasing in the sense that for any $n \in \mathbb{N}$,

$$\text{sdp}_n[A, \mathcal{F}] \geq \text{sdp}_{n+1}[A, \mathcal{F}]. \tag{34}$$

The following theorem summarizes the relationship between $p^*[A, \mathcal{F}]$ and the sequence of SDPs $\text{sdp}[A, \mathcal{F}]$.

Theorem 2.2. *Using the notation in this section, we have for all $n \geq 1$,*

$$p^*[A, \mathcal{F}] \leq \text{sdp}_n[A, \mathcal{F}]. \tag{35}$$

Moreover, if the set of constraints \mathcal{F} satisfies (19), then

$$p^*[A, \mathcal{F}] = \lim_{n \rightarrow \infty} \text{sdp}_n[A, \mathcal{F}]. \tag{36}$$

Proof. The inequality (35) was proved above for finite-dimensional Hilbert spaces. For the general case see Appendix A.1. For (36), a self-contained proof can be found in Appendix A.2. The convergence also follows from the convergence of the NPA hierarchy (20) together with Proposition 2.3. \square

We now discuss the first level relaxation of our new hierarchy (32) in more detail.

2.4. First Level Relaxation. For applications the first level relaxation often already gives good bounds. We find

$$\begin{aligned}
 \text{sdp}_1[A, \mathcal{F}] &= \underset{\Omega^1}{\text{maximize}} \quad \sum_{\alpha, \beta} A_{\alpha, \beta} \Omega_{(\alpha), (\beta)}^1 \\
 &\text{subject to} \quad \Omega^1 \in \text{Pos}(1 + N + M) \\
 &\quad \Omega_{\emptyset, \emptyset}^1 = 1 \\
 &\quad \sum_{i, j=0}^{N+M} f^i \bar{f}^j \Omega_{(i), (j)}^1 \geq 0 \quad \forall f, \bar{f} \in \mathcal{F}.
 \end{aligned}
 \tag{37}$$

Compared to this, the first level relaxation of the NPA hierarchy (16) gives

$$\begin{aligned}
 \tilde{\text{sdp}}_1[A, \mathcal{F}] &= \underset{\tilde{\Omega}^1}{\text{maximize}} \quad \sum_{\alpha, \beta} A_{\alpha, \beta} \tilde{\Omega}_{(\alpha), (\beta)}^1 \\
 &\text{subject to} \quad \tilde{\Omega}^1 \in \text{Pos}(1 + N + M) \\
 &\quad \tilde{\Omega}_{\emptyset, \emptyset}^1 = 1 \\
 &\quad \sum_{i=0}^{N+M} f^i \tilde{\Omega}_{(i), \emptyset}^1 \geq 0 \quad \forall f \in \mathcal{F}.
 \end{aligned}
 \tag{38}$$

By inspection we find that (37) has extra constraints compared to (38). This implies in particular that the first level of our hierarchy is never a worse approximation than the first level of the NPA hierarchy,

$$\text{sdp}_1[A, \mathcal{F}] \leq \tilde{\text{sdp}}_1[A, \mathcal{F}]. \tag{39}$$

The extra conditions are of the form

$$(40) \quad \sum_{i,j=0}^{N+M} g^i \bar{g}^j \Omega_{(i),(j)}^1 \geq 0 \quad \forall g, \bar{g} \in \mathcal{G} \quad \sum_{i,j=0}^{N+M} k^i \bar{k}^j \Omega_{(i),(j)}^1 \geq 0 \quad \forall k, \bar{k} \in \mathcal{K}$$

$$(41) \quad \sum_{i,j=0}^{N+M} g^i k^j \Omega_{(i),(j)}^1 \geq 0 \quad \forall g \in \mathcal{G}, \forall k \in \mathcal{K}.$$

We note that in many settings the constraint (41) can be inferred from the second level of the NPA hierarchy and hence can be added to the first NPA level as needed when evaluating examples. The former conditions (40) however are qualitatively different from the NPA hierarchy. We will see later that for certain applications and examples the additional conditions (40) are useful (Section 3). In the following section we compare the higher levels of the two hierarchies.

2.5. Comparison of Hierarchies.

Proposition 2.3. As seen in (37) and (38) we have

$$(42) \quad \text{sdp}_1[A, \mathcal{F}] \leq \tilde{\text{sdp}}_1[A, \mathcal{F}].$$

Moreover, for $n \geq 2$ we have

$$(43) \quad \text{sdp}_{2n}[A, \mathcal{F}] \leq \tilde{\text{sdp}}_n[A, \mathcal{F}].$$

Proof. Let Ω^{2n} be a feasible solution for $\text{sdp}_{2n}[A, \mathcal{F}]$ with the odd level constraints as in (33). For any $w \in \Sigma_{2n}$, let w_z and w_y be the subwords of w containing only symbols of type z and y respectively. For example, if $w = z_1 y_1^2 y_2 z_3 y_1$, then $w_z = z_1 z_3$ and $w_y = y_1^2 y_2 y_1$.

We define for every $w \in \Sigma_{2n}$, the complex number $m_w := \Omega_{w_z, w_y}^{2n}$ and let $\tilde{\Omega}_{u,v}^n = m_{u^* \circ v}$. Because of this form, it is easily seen that $\tilde{\Omega}_{u,v^* \circ w}^n = \tilde{\Omega}_{v \circ u, w}^n$. Moreover, observe $w \sim w'$ and then $w_z = w'_z$ as well as $w_y = w'_y$. It follows that $\tilde{\Omega}_{u,v}^n = \tilde{\Omega}_{u',v'}^n$ if $u \sim u'$ and $v \sim v'$. For the positivity constraint we write

$$(44) \quad \tilde{\Omega}^n = \sum_{u,v \in \Sigma_n} \tilde{\Omega}_{u,v}^n |u\rangle \langle v| = \sum_{u,v \in \Sigma_n} \Omega_{u_z^* \circ v_z, u_y^* \circ v_y}^{2n} |u\rangle \langle v|.$$

This matrix is a principal submatrix of the matrix

$$(45) \quad \sum_{s,t,u,v \in \Sigma_n} \Omega_{s^* \circ t, u^* \circ v} |s\rangle \langle t| \otimes |u\rangle \langle v|,$$

by only considering rows corresponding to t and s being words with only symbols of type z , and u and v being words with only symbols of type y , and also such that $\ell(s \circ u), \ell(t \circ v) \leq n$. As a result $\tilde{\Omega}^n \geq 0$. For the constraints $g \in \mathcal{G}$, we have

$$(46) \quad \sum_i g^i \sum_{u,v \in \Sigma_{n-1}} \tilde{\Omega}_{u,(i) \circ v}^n |u\rangle \langle v| = \sum_i g^i \sum_{u,v \in \Sigma_{n-1}} \Omega_{u_z^* \circ (i) \circ v_z, u_y^* \circ v_y}^{2n} |u\rangle \langle v|,$$

which again is a positive semidefinite matrix as it is a principal submatrix of $\Omega^{2n}[g]$. The positivity of $\tilde{\Omega}^n[k]$ for $k \in \mathcal{K}$ is similar. \square

This proposition implies in particular that the convergence of the new hierarchy $\text{sdp}_n[A, \mathcal{F}]$ already follows from the convergence of the NPA hierarchy $\text{sdp}_n[A, \mathcal{F}]$ (see Appendix A.2 for a direct proof). We leave it as an open question if the comparison $\text{sdp}_1[A, \mathcal{F}] \leq \tilde{\text{sdp}}_1[A, \mathcal{F}]$ for the first level is special or if we might even have $\text{sdp}_n[A, \mathcal{F}] \leq \tilde{\text{sdp}}_n[A, \mathcal{F}]$ in general.

3. APPLICATIONS

3.1. Two-Prover Games. In a two-prover game, each player (or prover) gets asked a question by the referee: $q_1 \in Q_1$ for the first player and $q_2 \in Q_2$ for the second player. Each player is then asked to provide an answer $a_1 \in A_1$ and $a_2 \in A_2$. The referee, looking at the questions and answers q_1, q_2, a_1, a_2 decides whether the players win or lose the game according to a function $V : A_1 \times A_2 \times Q_1 \times Q_2 \rightarrow \{0, 1\}$. The players may use any agreed upon protocol but they cannot communicate once they have received the questions. The fundamental quantity of interest given such a game is the largest probability of success that the players can achieve. The study of multi-prover games was introduced in [4] and has played a major role in theoretical computer science [1]. It also provides a very nice interpretation for

understanding nonlocal correlations that can be obtained by measuring an entangled state [16]. The value of a game defined by the verification predicate V and a distribution π is given by

$$\begin{aligned}
 \omega(V, \pi) := & \underset{(e,d)}{\text{maximize}} \quad \sum_{q_1, q_2} \pi(q_1, q_2) \sum_{a_1, a_2} V(a_1, a_2, q_1, q_2) e(a_1|q_1) d(a_2|q_2) \\
 \text{subject to} \quad & \sum_{a_1} e(a_1|q_1) = 1 \quad \forall q_1 \in Q_1 \\
 & \sum_{a_2} d(a_2|q_2) = 1 \quad \forall q_2 \in Q_2 \\
 & 0 \leq e(a_1|q_1) \leq 1 \quad \forall (a_1, q_1) \in A_1 \times Q_1 \\
 & 0 \leq d(a_2|q_2) \leq 1 \quad \forall (a_2, q_2) \in A_2 \times Q_2.
 \end{aligned} \tag{47}$$

In the notation of (3), we have $N = |Q_1||A_1|$, $M = |Q_2||A_2|$, $\alpha \in Q_1 \times A_1$ and $\beta \in Q_2 \times A_2$. The matrix specifying the objective function is given by

$$A_{(q_1, a_1), (q_2, a_2)} = \pi(q_1, q_2) V(a_1, a_2, q_1, q_2). \tag{48}$$

The constraints functions \mathcal{F} are the positivity and normalization conditions. When the players are allowed to share entanglement, then we define the entangled value of the game as

$$\begin{aligned}
 \omega^*(V, \pi) := & \underset{(\mathcal{H}, \psi, E, D)}{\text{maximize}} \quad \sum_{q_1, q_2} \pi(q_1, q_2) \sum_{a_1, a_2} V(a_1, a_2, q_1, q_2) \langle \psi | E(a_1|q_1) D(a_2|q_2) | \psi \rangle \\
 \text{subject to} \quad & [E(a_1|q_1), D(a_2|q_2)] = 0, \quad \forall a_1, a_2, q_1, q_2 \in A_1 \times A_2 \times Q_1 \times Q_2 \\
 & \sum_{a_1} E(a_1|q_1) = \text{id}_{\mathcal{H}} \quad \forall q_1 \in Q_1 \\
 & \sum_{a_2} D(a_2|q_2) = \text{id}_{\mathcal{H}} \quad \forall q_2 \in Q_2 \\
 & 0 \leq E(a_1|q_1) \leq \text{id}_{\mathcal{H}} \quad \forall (a_1, q_1) \in A_1 \times Q_1 \\
 & 0 \leq D(a_2|q_2) \leq \text{id}_{\mathcal{H}} \quad \forall (a_2, q_2) \in A_2 \times Q_2.
 \end{aligned} \tag{49}$$

Using the procedure described in Section 2, we can define a sequence of SDPs $\omega^{\text{sdp}_n}(V, \pi)$ that are upper bounds on $\omega^*(V, \pi)$. In particular, for $n = 1$, the SDP reads

$$\begin{aligned}
 \omega^{\text{sdp}_1}(V, \pi) := & \underset{\Omega^1}{\text{maximize}} \quad \sum_{q_1, q_2} \pi(q_1, q_2) \sum_{a_1, a_2} V(a_1, a_2, q_1, q_2) \Omega_{(q_1, a_1), (q_2, a_2)}^1 \\
 \text{subject to} \quad & \Omega^1 \in \text{Pos}(1 + |Q_1||A_1| + |Q_2||A_2|) \\
 & \sum_{a_1} \Omega_{(q_1, a_1), u}^1 = \Omega_{\emptyset, u}^1 \quad \forall q_1 \in Q_1, u \in \Sigma_1 \\
 & \sum_{a_2} \Omega_{(q_2, a_2), u}^1 = \Omega_{\emptyset, u}^1 \quad \forall q_2 \in Q_2, u \in \Sigma_1 \\
 & \Omega_{u, v}^1 \geq 0 \quad \forall u, v \in \Sigma_1.
 \end{aligned} \tag{50}$$

Compared to the first level of the NPA hierarchy, the additional constraint is the last one, namely that all the matrix entries are nonnegative. Note that for the special case of two-prover games the NPA hierarchy would explicitly encode the fact that we can assume that the operators $E(a_1|q_1)$ and $D(a_2|q_2)$ define projective measurements [36]. This is done by adding some relations in the algebra Σ_∞ : one would add the relation,²

$$(q_i, a_i) \circ (q_i, a'_i) = \delta_{a_i=a'_i} (q_i, a_i) \quad \text{for } i \in \{1, 2\}, \tag{51}$$

and this decreases the number of words to be considered. Using this property together with the second level of the NPA hierarchy, one could then add to the first level of NPA the constraint that the off-diagonal blocks of the matrix $\tilde{\Omega}^1$ only have nonnegative elements:

$$\tilde{\Omega}_{(q_1, a_1), (q_2, a_2)}^1 \geq 0 \quad \text{for all } (q_1, a_1) \in Q_1 \times A_1 \quad \text{and} \quad (q_2, a_2) \in Q_2 \times A_2. \tag{52}$$

The SDP with these nonnegativity constraints for the off-diagonal blocks also appeared in the context of studying unique games in [31] (see also [29] for a discussion of various SDP relaxations). The

²We could easily add this property as well, but we choose not to do it to simplify the exposition.

additional constraint in our SDP is that all the entries of the matrix Ω^1 are required to be nonnegative.

Independent work: Very recently and independently of our work, the preprint [47] appeared showing (among other things) that in the case of games, the first level of the NPA hierarchy can be strengthened by including the constraint that the matrix elements are nonnegative. This strengthening corresponds to ω^{sdp_1} as in (50).

3.2. Noisy Channel Coding. Let us recall the setup of channel coding from the introduction. We have a channel mapping an element from the set X to an element of the set Y according to probabilities given by $W_{X \rightarrow Y}(y|x)$. The objective is to determine the maximum success probability for transmitting k bits of information using this channel. The classical version of the problem is described in (1). In the notation of (3), we have $N = 2^k|X|$, $M = 2^k|Y|$, $\alpha \in [2^k] \times X$ and $\beta \in [2^k] \times Y$. The matrix specifying the objective function is given by

$$(53) \quad A_{(i,x),(j,y)} = \delta_{i=j} W_{X \rightarrow Y}(y|x).$$

The constraints functions \mathcal{F} are the positivity and normalization conditions. Explicitly writing the first level SDP from (37) with some easy simplifications, we get

$$(54) \quad \begin{aligned} \text{S}^{\text{sdp}_1}(W, k) &:= \underset{\Omega^1}{\text{maximize}} \quad \frac{1}{2^k} \sum_{x,y,i} W_{X \rightarrow Y}(y|x) \Omega_{(i,x),(i,y)}^1 \\ &\text{subject to} \quad \Omega^1 \in \text{Pos}(1 + k|X| + k|Y|) \\ &\quad \Omega_{\emptyset, \emptyset}^1 = 1 \\ &\quad \sum_x \Omega_{w,(i,x)}^1 = \Omega_{w,\emptyset}^1 \quad \forall i \in [2^k], w \in \Sigma_1 \\ &\quad \sum_i \Omega_{w,(i,y)}^1 = \Omega_{w,\emptyset}^1 \quad \forall y \in Y, w \in \Sigma_1 \\ &\quad \Omega_{u,v}^1 \geq 0 \quad \forall u, v \in \Sigma_1. \end{aligned}$$

Again, the additional constraint compared to the NPA hierarchy is the last one, namely the fact that all the entries of Ω^1 are nonnegative. Using this condition, we see that we have the desirable property that for any valid channel W and any k ,

$$(55) \quad \text{S}^{\text{sdp}_1}(W, k) \leq \frac{1}{2^k} \sum_{x,y,i} W_{X \rightarrow Y}(y|x) \Omega_{(i,x),\emptyset}^1 = \frac{1}{2^k} \sum_i \Omega_{\emptyset,\emptyset}^1 = 1.$$

Now as a concrete example for which the classical and the quantum success probabilities are different we mention the following setup from [43]. The objective is to send $k = 1$ bit over the noisy channel $Z_{X \rightarrow Y}(y|x)$ represented by the input-output matrix

$$(56) \quad \begin{pmatrix} 1/3 & 1/3 & 0 & 0 \\ 0 & 0 & 1/3 & 1/3 \\ 1/3 & 0 & 1/3 & 0 \\ 0 & 1/3 & 0 & 1/3 \\ 1/3 & 0 & 0 & 1/3 \\ 0 & 1/3 & 1/3 & 0 \end{pmatrix}.$$

It is shown in [43] that for this channel the classical and quantum success probability as in (1) and (2) respectively are separated as,

$$(57) \quad S^*(Z, 1) \geq \frac{2 + 2^{-1/2}}{3} \approx 0.902 > 0.833 \approx \frac{5}{6} = S(Z, 1).$$

Moreover, it was shown in [27, 52] that the above lower bound for $S^*(W, 1)$ is optimal as long as we restrict the optimization in (2) to two dimensional Hilbert spaces.

Implementing our first level SDP relaxation (54) using CVX for MATLAB [25, 24] gives the first non-trivial upper bound for the general optimization (2) leading to,³

$$(58) \quad \text{S}^{\text{sdp}_1}(Z, 1) \approx 0.908 \geq S^*(Z, 1) \geq 0.902.$$

We note that the first level NPA relaxation as in (38) only gives the trivial upper bound of one. This is the case even when adding the constraint that the off-diagonal elements of the matrix $\tilde{\Omega}_{(i,x),(j,y)}^1$ are

³The code is available at <http://www.omarfawzi.info>.

nonnegative.⁴ In Appendix C, we show that the bound given by the $S^{\text{sdP}_1}(Z, 1)$ is in fact achievable with four dimensional entanglement assistance:

$$(59) \quad S^*(Z, 1) \geq \frac{1}{2} + \frac{1}{\sqrt{6}} \approx 0.908.$$

Subsequent work: After this work was posted, a limit on the maximum advantage that can be obtained by using entanglement assistance was proved in [2]. More precisely, we have that for any channel W and sending k bits of information,

$$(60) \quad S(W, k) \geq (1 - e^{-1})S^*(W, k).$$

3.3. Randomness Extractors. A randomness extractor is defined by a set of functions

$$(61) \quad \text{Ext} := \left\{ f_s : [2^n] \rightarrow [2^m] \right\}_{s \in [2^d]}$$

mapping bit strings of length n to shorter ones of length m ; see [51] for a survey. As the name suggests, the goal is to extract (almost) perfect randomness from a weaker source of randomness. That is, given some distribution over bit strings of length n , by applying one of the functions chosen uniformly at random, we want to obtain a distribution close to the uniform one (in the total variation distance). The requirement is that the initial distribution contains enough randomness as measured using the min-entropy which is equal to minus the logarithm of the maximal entry of the probability distribution. In order for this procedure to work for all sources satisfying the min-entropy constraint, it can be shown that the minimal size of the seed d is logarithmic in n [51]. Since the total variation distance between two distributions can itself be written as an optimization over test functions, the performance of a given extractor Ext can be cast as a bilinear optimization program. The objective function in the general program (3) is chosen to be indexed by elements $i \in [2^n]$ and pairs $(s, j) \in [2^{d+m}]$,

$$(62) \quad A_{i,(s,j)} := \frac{1}{2^d} \delta_{f_s(i)=j} - \frac{1}{2^{d+m}}.$$

The constraints are the positivity and normalization of the input distribution z_i , as well as the min-entropy requirement, and the restriction to test functions as given by positive numbers $y_{(s,j)}$. We arrive at

$$(63) \quad \begin{aligned} \text{Err}(\text{Ext}, k) &:= \underset{(z_i, y_{(s,j)})}{\text{maximize}} && \frac{1}{2^d} \sum_{i,(s,j)} \left[\delta_{f_s(i)=j} - \frac{1}{2^m} \right] z_i y_{(s,j)} \\ &\text{subject to} && 0 \leq z_i \leq 2^{-k} \quad \forall i \in [2^n] \\ &&& \sum_i z_i = 1 \\ &&& 0 \leq y_{(s,j)} \leq 1 \quad \forall (s, j) \in [2^{d+m}]. \end{aligned}$$

Here, the parameter k measures the amount of initial min-entropy. As discussed before, the constraints on the positive numbers $y_{(s,j)}$ just ensure that it is a test function, and hence the program becomes

$$(64) \quad \begin{aligned} \text{Err}(\text{Ext}, k) &= \underset{z_i}{\text{maximize}} && \frac{1}{2} \cdot \frac{1}{2^d} \sum_{(s,j)} \left| \sum_i \delta_{f_s(i)=j} z_i - \frac{1}{2^m} \right| \\ &\text{subject to} && 0 \leq z_i \leq 2^{-k} \quad \forall i \in [2^n] \\ &&& \sum_i z_i = 1, \end{aligned}$$

the total variation distance of the output distribution to the uniform distribution on m bits. The average over the choice of the seed value s outside of the absolute value ensures that the closeness to the uniform distribution holds even conditioned on the seed. We also call

$$(65) \quad C(\text{Ext}, k) := \text{Err}(\text{Ext}, k)$$

⁴Another upper bound, the so-called non-signaling success probability of the channel (56), is one as well (see [43, 27, 52] for details).

the classical value of Ext . We can now apply our general quantization procedure to (63). Assuming for simplicity that the underlying Hilbert space is of finite dimensions and repeating the steps (22) - (24), we arrive at the program (for the general case see again Appendix A.1),

$$\begin{aligned}
(66) \quad \text{Err}^*(\text{Ext}, k) := & \underset{(\sigma, E_i, D_{(s,j)})}{\text{maximize}} \quad \frac{1}{2^d} \sum_{i, (s,j)} \left[\delta_{f_s(i)=j} - \frac{1}{2^m} \right] \text{Tr} \left[E_i \sigma^{1/2} D_{(s,j)} \sigma^{1/2} \right] \\
& \text{subject to} \quad \sigma \geq 0, \text{Tr}[\sigma] = 1 \\
& 0 \leq E_i \leq 2^{-k} \mathbb{1} \quad \forall i \in [2^n] \\
& \sum_i E_i = \mathbb{1} \\
& 0 \leq D_{(s,j)} \leq \mathbb{1} \quad \forall (s, j) \in [2^{d+m}].
\end{aligned}$$

Setting $\sigma_i := \sigma^{1/2} E_i \sigma^{1/2}$ and again by the duality of the 1-norm to the ∞ -norm we can rewrite the program as

$$\begin{aligned}
(67) \quad \text{Err}^*(\text{Ext}, k) = & \underset{\sigma_i}{\text{maximize}} \quad \frac{1}{2} \cdot \frac{1}{2^d} \sum_{(s,j)} \left\| \sum_i \left[\delta_{f_s(i)=j} - \frac{1}{2^m} \right] \sigma_i \right\|_1 \\
& \text{subject to} \quad 0 \leq \sigma_i \leq 2^{-k} \sum_i \sigma_i \quad \forall i \in [2^n] \\
& \sum_i \text{Tr}[\sigma_i] = 1.
\end{aligned}$$

From this we define the normalized classical-quantum state

$$(68) \quad \sigma := \sum_i |i\rangle\langle i| \otimes \sigma_i \quad \text{satisfying} \quad \sigma \leq 2^{-k} \cdot \mathbb{1} \otimes \left(\sum_i \sigma_i \right),$$

and hence the objective function in (67) corresponds to the total variation distance of the output to a quantum state that is of the form uniform distribution on m bits tensor the reduced state on the quantum system. This means that an adversary cannot tell the output apart from the uniform distribution even when having access to the quantum system as well as the value of the seed. Here, the inequality condition in (68) defines the worst case quantum conditional min-entropy that is, e.g., discussed in [50, Appendix B]. However, in the literature the average case quantum conditional min-entropy is more commonly used (as discussed in [44]). This gives rise to the following so-called quantum value of Ext ,

$$\begin{aligned}
(69) \quad Q(\text{Ext}, k) := & \underset{(\sigma_i, \omega)}{\text{maximize}} \quad \frac{1}{2} \cdot \frac{1}{2^d} \sum_{i, (s,j)} \left\| \sum_i \left[\delta_{f_s(i)=j} - \frac{1}{2^m} \right] \sigma_i \right\|_1 \\
& \text{subject to} \quad \omega \geq 0, \text{Tr}[\omega] = 1 \\
& 0 \leq \sigma_i \leq 2^{-k} \omega \quad \forall i \in [2^n] \\
& \sum_i \text{Tr}[\sigma_i] = 1.
\end{aligned}$$

However, it follows from the equivalence of the worst case and average case quantum conditional min-entropy [50, Lemma 20] that there cannot be a large gap between Err^* and Q .

Proposition 3.1. *For $\varepsilon > 0$ we have*

$$(70) \quad Q(\text{Ext}, k) \leq \text{Err}^*(\text{Ext}, k - \log(1/\varepsilon^2 + 1)) + \varepsilon.$$

We conclude that $\text{Err}^*(\text{Ext}, k)$ captures to what extent Ext is a quantum-proof extractor. Hence, this property can be tested by our SDP hierarchy (32). We give the full first level $\text{Err}^{\text{sdp}_1}(\text{Ext}, k)$ as in (37) in Appendix D. For our purposes, however, it will be sufficient to work with the following

simplified upper bound $\text{Err}^{\overline{\text{sdp}_1}}(\text{Ext}, k) \geq \text{Err}^{\text{sdp}_1}(\text{Ext}, k)$ that ignores some of the constraints:

$$\begin{aligned}
 \text{Err}^{\overline{\text{sdp}_1}}(\text{Ext}, k) &:= \underset{\Omega^1}{\text{maximize}} \quad \frac{1}{2^d} \sum_{i, (s, j)} \left[\delta_{f_s(i)=j} - \frac{1}{2^m} \right] \Omega_{(i), (s, j)}^1 \\
 &\text{subject to} \quad \Omega^1 \in \text{Pos}(1 + 2^n + 2^{d+m}) \\
 &\quad \Omega_{w, w'}^1 \geq 0 \quad \forall w, w' \in \Sigma_1 \\
 &\quad \Omega_{\emptyset, \emptyset}^1 = 1, \quad \Omega_{\emptyset, w}^1 = \sum_i \Omega_{(i), w}^1 \quad \forall w \in \Sigma_1 \\
 &\quad 2^{-k} \Omega_{\emptyset, w}^1 \geq \Omega_{(i), w}^1 \quad \forall i \in [2^n], \quad \forall w \in \Sigma_1 \\
 &\quad \Omega_{\emptyset, w}^1 \geq \Omega_{(s, j), w}^1 \quad \forall (s, j) \in [2^{d+m}], \quad \forall w \in \Sigma_1,
 \end{aligned} \tag{71}$$

where again some of the positivity constraints on the matrix elements are new as compared to the NPA hierarchy. We emphasize that these conditions are important to obtain the following bounds on the gap between $\text{Err}(\text{Ext}, k)$ and $\text{Err}^{\overline{\text{sdp}_1}}(\text{Ext}, k)$, which then also give an upper estimate for the error of the quantum-proof extractor (66).

Theorem 3.2. *We have that*

$$\text{Err}^{\overline{\text{sdp}_1}}(\text{Ext}, k) \leq \sqrt{2} \sqrt{2^m} \sqrt{\text{Err}(\text{Ext}, k)}, \tag{72}$$

as well as

$$\text{Err}^{\overline{\text{sdp}_1}}(\text{Ext}, k) \leq 6 K_G 2^{n-k} \text{Err}(\text{Ext}, k - 1) \tag{73}$$

where K_G denotes Grothendieck's constant.

The proof is based on ideas from [9, Theorem 5] and we present it in full detail in Appendix D. We remark that compared to the relaxation in [9, Theorem 4], the SDP relaxation (71) has some new and different constraints. The additional constraints are introduced by the sub-matrices where one variable is equal to the empty word \emptyset . Using these additional constraints we have the desirable property that the first level SDP relaxation $\text{Err}^{\overline{\text{sdp}_1}}(\text{Ext}, k)$ is always bounded by one,⁵

$$\text{Err}^{\overline{\text{sdp}_1}}(\text{Ext}, k) \leq \frac{1}{2^d} \sum_{i, (s, j): f_s(i)=j} \left(1 - \frac{1}{2^m} \right) \Omega_{(i), (s, j)}^1 \leq \frac{1}{2^d} \sum_{i, s} \left(1 - \frac{1}{2^m} \right) \Omega_{(i), \emptyset}^1 = 1 - \frac{1}{2^m}. \tag{74}$$

This implies that the argument in [9, Theorem 8] showing a large gap between the SDP value and the quantum value does not apply for $\text{Err}^{\overline{\text{sdp}_1}}(\text{Ext}, k)$. We leave it as an open question whether there can be a large gap between $\text{Err}^{\overline{\text{sdp}_1}}(\text{Ext}, k)$ or $\text{Err}^{\text{sdp}_1}(\text{Ext}, k)$ and $\text{Err}^*(\text{Ext}, k)$.⁶

Finally, we point out that using ideas similar to the ones presented in this section, one can also construct a hierarchy for more general objects called quantum-proof randomness condensers [51, 8]. It would be interesting to explore in more detail the applications of these relaxations to condensers.

3.4. Optimization over the cone \mathcal{CS}_+ . Here we show that one can use the hierarchy introduced in Section 2 to give a SDP hierarchy of outer approximation for the cone \mathcal{CS}_+^N defined in [34],

$$\mathcal{CS}_+^N := \left\{ \Gamma \in \text{Pos}(N) : \Gamma_{\alpha, \beta} = \text{Tr}[X_\alpha X_\beta] \text{ with } X_1, \dots, X_N \in \text{Pos}(d) \text{ for some } d \in \mathbb{N} \right\}. \tag{75}$$

A typical program considered by Burgdorf, Laurent and Piovesan [13] now reads as follows:

$$\begin{aligned}
 p^{\mathcal{CS}_+} [A, \{F^i\}_i] &:= \underset{\Lambda}{\text{maximize}} \quad \sum_{\alpha, \beta} A_{\alpha, \beta} \Lambda_{\alpha, \beta} \\
 &\text{subject to} \quad \Lambda \in \mathcal{CS}_+^N \\
 &\quad \sum_{\alpha, \beta} F_{\alpha\beta}^i \Lambda_{\alpha, \beta} = 0 \quad \forall i.
 \end{aligned} \tag{76}$$

⁵Both $\text{Err}^*(\text{Ext}, k)$ and $Q(\text{Ext}, k)$ are always bounded by one whereas the relaxation in [9, Theorem 4] can get arbitrarily large in general.

⁶Some more results on how to extend the argument in [9, Theorem 8] to other SDP relaxations can be found in [20].

Here again, $A_{\alpha,\beta}$ are real numbers specifying the objective function, and the real numbers $F_{\alpha,\beta}^i$ specify additional equality constraints. Specific instances include the quantum versions of stability and chromatic numbers for graphs; see e.g., [14, 13]. As usual it is important to ensure that the matrices X_i in the factorization are bounded (for convergence of the hierarchy). So we assume that the constraints F^i are such that the diagonal entries $\Lambda_{\alpha,\alpha}$ of any feasible solution are bounded. For applications, this is always satisfied. Note that as we do not distinguish between two types of variables here, we use N instead of $N + M$ for the number of variables.

Following the procedure given in Section 2, the n -th level SDP relaxation is given by optimizing over a positive semidefinite matrix Ω^n whose rows and columns are indexed by words of length up to n on the alphabet $\{1, \dots, N\}$. These words span a the complex linear subspace of Σ_∞ which we denote by Σ_n . The entries $\Omega_{(\alpha),(\beta)}$ corresponding to words of length 1 are the candidate entries for $\Lambda_{\alpha,\beta}$ in the program (76). The fact that $\Lambda \in \mathcal{CS}_+^N$ allows us to add additional constraints as described in (31). When n is odd and writing

$$(77) \quad \delta = \frac{N^{n+1} - 1}{N - 1} \quad \text{and} \quad \delta' = \left(\frac{N^{(n-1)/2+1} - 1}{N - 1} \right)^2,$$

we find

$$(78) \quad \begin{aligned} \text{sdp}_n[A, \{F^i\}_i] &:= \underset{\Omega^n}{\text{maximize}} \quad \sum_{\alpha,\beta} A_{\alpha,\beta} \Omega_{(\alpha),(\beta)}^n \\ &\text{subject to} \quad \Omega^n \in \text{Pos}(\delta) \\ &\quad \Omega_{\emptyset,\emptyset}^n = 1 \\ &\quad \sum_{r,s,u,v \in \Sigma_{(n-1)/2}} \Omega_{r^* \circ (\alpha) \circ s, u^* \circ (\beta) \circ v}^n |r\rangle\langle s| \otimes |u\rangle\langle v| \in \text{Pos}(\delta') \quad \forall \alpha, \beta \in [N] \\ &\quad \Omega_{(\alpha) \circ u, v \circ (\beta)}^n = \Omega_{u \circ (\beta), (\alpha) \circ u}^n \quad \forall \alpha, \beta \in [N], u, v \in \Sigma_{n-1} \\ &\quad \sum_{\alpha,\beta} F_{\alpha\beta}^i \Omega_{(\alpha),(\beta)}^n = 0. \end{aligned}$$

Recall that \circ denotes the concatenation of words and (α) refers to a word of length 1 with the symbol α . Note that $n = 1$ corresponds to optimizing over the doubly nonnegative cone. The way we constructed $\text{sdp}_n[A, \{F^i\}_i]$ as a relaxation of $p[A, \{F^i\}_i]$ is similar to what we did in previous sections. Let $\Lambda \in \mathcal{CS}_+^N$, then there exists positive semidefinite matrices $X'_1, \dots, X'_N \in \text{Pos}(d)$ such that $\Gamma_{\alpha,\beta} = \text{Tr}[X'_\alpha X'_\beta]$. First, let us write $X_\alpha = \sqrt{d} X'_\alpha$ and for any word $u \in \Sigma_n$, X_u as the product of the matrices corresponding to its symbols: $X_u = X_{u_1} \cdots X_{u_n}$ with $X_\emptyset = \mathbb{1}$. Recalling that u^* is the word u inverted, we define

$$(79) \quad \Omega_{u,v}^n := \text{Tr} \left[\frac{\mathbb{1}}{d} \cdot X_{u^*} X_v \right].$$

First, as Ω^n is the (scaled) Gram matrix of the family $\{X_u : u \in \Sigma_n\}$, it is positive semidefinite. Also $\Omega_{1,1}^n = \text{Tr}[\mathbb{1}/d] = 1$. Moreover, for a vector $|\phi\rangle = \sum_{r,u} c_{r,u} |r\rangle|u\rangle$, we have

$$(80) \quad \begin{aligned} \langle \phi | &\sum_{r,s,u,v \in \Sigma_{(n-1)/2}} d \cdot \Omega_{r^* \circ (\alpha) \circ s, u^* \circ (\beta) \circ v}^n |r\rangle\langle s| \otimes |u\rangle\langle v| \phi \rangle \\ &= \sum_{r,s,u,v} \bar{c}_{r,u} c_{s,v} \text{Tr} \left[X_{s^*} X_\alpha X_r X_{u^*} X_\beta X_v \right] \end{aligned}$$

$$(81) \quad = \text{Tr} \left[\left(\sum_{s,v} c_{s,v} X_v X_{s^*} \right) X_\alpha \left(\sum_{r,u} \bar{c}_{r,u} X_r X_{u^*} \right) X_\beta \right]$$

$$(82) \quad = \text{Tr} \left[\left(\sum_{s,v} c_{s,v} X_v X_{s^*} \right) X_\alpha \left(\sum_{s,v} c_{s,v} X_v X_{s^*} \right)^* X_\beta \right] \geq 0.$$

The constraint

$$(83) \quad \Omega_{(\alpha) \circ u, v \circ (\beta)}^n = \Omega_{u \circ (\beta), (\alpha) \circ u}^n$$

corresponds to the cyclicity of the trace,

$$(84) \quad d \cdot \Omega_{(\alpha) \circ u, v \circ (\beta)}^n = \text{Tr} \left[X_{u^*} X_{\alpha} X_v X_{\beta} \right] = \text{Tr} \left[X_{\beta} X_{u^*} X_{\alpha} X_v \right] = d \cdot \Omega_{u \circ (\beta), (\alpha) \circ v}^n.$$

Note that such a constraint did not appear in our other examples as we were optimizing over the state involved in defining Ω^n . In this example, we want to fix the state to be maximally mixed, $1/d$, and this is reflected in the cyclicity condition. We can also define the SDPs for even n similarly as in (33).

We implemented the SDP relaxations to test whether a given matrix K is in \mathcal{CS}_+ . In [21, 34] it was shown that the matrix

$$(85) \quad K := \begin{pmatrix} 4 & 0 & 2 & 2 & 0 \\ 0 & 4 & 0 & 2 & 2 \\ 2 & 0 & 4 & 0 & 3 \\ 2 & 2 & 0 & 4 & 0 \\ 0 & 2 & 3 & 0 & 4 \end{pmatrix}$$

is not in the closure of \mathcal{CS}_+ . Using CVX for MATLAB [25, 24], we were able to numerically certify using level $n = 3$ of the hierarchy that the matrix is indeed not in the cone \mathcal{CS}_+ .⁷

The convergence proof of Theorem 2.2 covers the above case as well, which then raises the question how the limiting point

$$(86) \quad p^*[A, \{F^i\}_i] := \lim_{n \rightarrow \infty} \text{sdp}_n[A, \{F^i\}_i]$$

of the programs (78) can be represented. Not surprisingly, we cannot assert that it corresponds to an element in the cone \mathcal{CS}_+ which asks for an underlying finite-dimensional Hilbert space. However, as shown in the Appendix B, the assumption that Connes' embedding conjecture [38, 17] has a positive answer implies that the value $p^*[A, \{F^i\}_i]$ agrees with the program (76), or more precisely, with its value if optimized over the closure $\overline{\mathcal{CS}}_+$ of the cone \mathcal{CS}_+ .⁸

Corollary 3.3. *For any $n \geq 1$ we have*

$$(87) \quad p^{\mathcal{CS}_+}[A, \{F^i\}_i] \leq \text{sdp}_n[A, \{F^i\}_i].$$

Moreover, provided the Connes embedding conjecture has a positive answer [17, 38], we have

$$(88) \quad p^{\overline{\mathcal{CS}}_+}[A, \{F^i\}_i] = p^*[A, \{F^i\}_i].$$

In order to prove (88), we may use Appendix A.2, as well as make use of the cyclicity of the trace to show that the state constructed there actually corresponds to a tracial state. We present such an argument in Appendix B.2. Alternatively, we could again make use of the fact that our hierarchy converges to the same value as the NPA hierarchy with added cyclicity constraints. These imply that the state τ constructed by the NPA convergence proof for Σ_{∞} is a tracial state, that is $\tau(ab) = \tau(ba)$. However, if Connes' embedding conjecture holds, then this state can be represented as a tracial state on the ultrapower of the hyperfinite factor. Finally, Burgdorf, Laurent and Piovesan [13] have shown that this implies the stated result.

APPENDIX A. MISSING PROOFS FOR GENERAL HILBERT SPACES

A.1. Upper Bounds on the Quantum Value. Here we show that even if we allow for general Hilbert spaces in the quantum program (7), than SDP hierarchy (32)-(33) is still a relaxation thereof (in Section 2.3 we have only shown this for finite-dimensional spaces). For this we start from the quantum program (7) and upper bound it in a more algebraic form.

Given any feasible solution $(\mathcal{H}, \psi, E_{\alpha}, D_{\beta})$ of the quantum program (7) we consider the algebra generated by the operators

$$(89) \quad D_1, \dots, D_M,$$

acting on the Hilbert space \mathcal{H} , and denote its closure in operator norm by \mathcal{D} . This is then a C^* -algebra and we denote the set of hermitian functionals on \mathcal{D} by \mathcal{D}_h^* and the set of positive functionals by \mathcal{D}_+^* . Now the normalized vector $\psi \in \mathcal{H}$ induces a normalized positive functional $\sigma \in \mathcal{D}_+^*$ via

$$(90) \quad \mathcal{D} \ni D \mapsto \sigma(D) := \langle \psi | D \psi \rangle.$$

⁷The code is available at <http://www.omarfawzi.info>.

⁸We write maximize in (76), which is consistent with the statement that the maximum is not attained (cf. Footnote 1). Clearly, the limiting point of our SDP hierarchy then corresponds to the supremum, and hence to the optimization over the closure of the cone \mathcal{CS}_+ .

Moreover, the hermitian operators E_α induce positive functionals $\rho_\alpha \in \mathcal{D}_h^*$,

$$(91) \quad \mathcal{D} \ni D \mapsto \rho_\alpha(D) := \langle \psi | E_\alpha D \psi \rangle = \langle \psi | E_\alpha^{1/2} D E_\alpha^{1/2} \psi \rangle,$$

where the last equality follows from the commutativity constraint $[E_\alpha, D_\beta] = 0$. In order to find an upper bound on the quantum value $p^*[A, \mathcal{F}]$, we consider the following optimization program over all C^* -algebras \mathcal{D} ,

$$(92) \quad \begin{aligned} \bar{p}[A, \mathcal{F}] &:= \underset{(\mathcal{D}, \rho_\alpha, D_\beta)}{\text{maximize}} && \sum_{\alpha, \beta} A_{\alpha, \beta} \rho_\alpha(D_\beta) \\ &\text{subject to} && \rho_\alpha \in \mathcal{D}_h^*, \sigma \in \mathcal{D}_+^* \text{ with } \sigma(\mathbb{1}) = 1 \\ &&& g(\rho_1, \dots, \rho_N, \sigma) \geq 0 \quad \forall g \in \mathcal{G} \\ &&& k(D_1, \dots, D_M) \geq 0 \quad \forall k \in \mathcal{K}, \end{aligned}$$

where the constraints $g \in \mathcal{G}$ are now understood as

$$(93) \quad g(\rho_1, \dots, \rho_N, \sigma) := g^0 \sigma + \sum_{\alpha \in [N]} g^\alpha \rho_\alpha,$$

and positivity is read in the algebraic sense. Note that the Archimedian constraints (19) translate to (which we always assume to be included in $\mathcal{G} \cup \mathcal{K}$),

$$(94) \quad \forall \alpha \in [N] : C\sigma \geq \rho_\alpha \geq -C\sigma \quad \text{and} \quad \forall \beta \in [M] : C\mathbb{1} \geq D_\beta \geq -C\mathbb{1}.$$

Now we show that the SDP hierarchy (32)-(33) is an upper bound on the algebraic program (92), and with that also on the quantum program (7).

Proposition A.1. *For any $n \in \mathbb{N}$ we have that,*⁹

$$(95) \quad \text{sdp}_n[A, \mathcal{F}] \geq \bar{p}[A, \mathcal{F}] \geq p^*[A, \mathcal{F}].$$

Proof. The second inequality follows from the discussion above and we now prove the first inequality.

Let ρ_α, σ be the set of functionals associated to the optimal solution $\bar{p}[A, \mathcal{F}]$. A standard GNS construction for the state σ gives rise to a Hilbert space \mathcal{H} , a dense mapping $i : \mathcal{D} \rightarrow \mathcal{H}$, a vector $\xi = i(\mathbb{1})$ and a representation $\pi : \mathcal{D} \rightarrow \mathcal{B}(\mathcal{H})$ defined by $\pi(x)i(a) = i(xa)$, such that

$$(96) \quad \langle i(a) | i(b) \rangle = \sigma(a^*b) \quad \text{and} \quad \sigma(x) = \langle \xi | \pi(x)\xi \rangle.$$

For the sake of convenience, we identify D_β with $\pi(D_\beta)$. By the von Neumann commutant theorem, the double commutant $\pi(\mathcal{D})''$ of $\pi(\mathcal{D})$ is a von Neumann algebra, denoted by \mathcal{M} , and the vector ξ defines a normal state on \mathcal{M} . Now, by [53, Theorem 2.2], there exists an anti-unitary operator $J : \mathcal{H} \rightarrow \mathcal{H}$, satisfying $J^2 = \mathbb{1}$, another vector $\psi \in \mathcal{H}$ (differing from ξ by at most a phase), such that for all $Y \in \mathcal{M}$

$$(97) \quad \langle \xi | Y \xi \rangle = \langle \psi | Y \psi \rangle, \quad J\psi = \psi, \quad \text{and} \quad \langle \psi | Y J Y \psi \rangle \geq 0.$$

Moreover, we have that $J\mathcal{M}J = \mathcal{M}'$, meaning that for any operator X in the commutant of \mathcal{M} there exists an element $Y \in \mathcal{M}$ such that $JYJ = X$. By the noncommutative Radon-Nikodym derivative argument, see, e.g., [49], setting

$$(98) \quad h_\alpha : \mathcal{H} \rightarrow \mathcal{H}, \quad \langle i(a) | h_\alpha i(b) \rangle = \rho_\alpha(a^*b)$$

defines an operator which is positive and bounded, since

$$(99) \quad 0 \leq \langle i(a) | h_\alpha i(a) \rangle = \rho_\alpha(a^*a) \leq C\sigma(a^*a) = C\langle i(a) | i(a) \rangle.$$

A standard calculation also gives that $h_\alpha \in \mathcal{M}'$. Moreover, for any linear constraint $g(\rho_1, \dots, \rho_N, \sigma) \geq 0$ we have

$$(100) \quad \langle i(a) | g(h_1, \dots, h_N, \mathbb{1}) i(a) \rangle = g(\langle i(a) | h_1 i(a) \rangle, \dots, \langle i(a) | h_N i(a) \rangle, \langle i(a) | i(a) \rangle)$$

$$(101) \quad = g(\rho_1, \dots, \rho_N, \sigma)(a^*a) \geq 0$$

and hence $g(h_1, \dots, h_N, \mathbb{1})$ defines a positive operator. By the previous assertions, we have that $E_\alpha = Jh_\alpha J$ is an element of \mathcal{M} and likewise $g(E_1, \dots, E_N, \mathbb{1}) \geq 0$.

⁹We will see in Appendix 2 that even $\bar{p}[A, \mathcal{F}] = p^*[A, \mathcal{F}]$.

We have all necessary ingredients at hand to define the analogue of the bilinear form $\omega : \Sigma_\infty \times \Sigma_\infty \rightarrow \mathbb{C}$ from (25). First, let us abbreviate for $\gamma \in \{1, \dots, N + M\}$

$$(102) \quad Z_\gamma := \begin{cases} X_\gamma : & k \in \{1, \dots, N\} \\ Y_{\gamma-N} : & k \in \{N + 1, \dots, N + M\} \end{cases},$$

and for any word $u = (u_1, \dots, u_\ell)$, $u_i \in \{1, \dots, N + M\}$,

$$(103) \quad Z_u := Z_{u_1} \dots Z_{u_\ell}.$$

For any two words u, v we set

$$(104) \quad \omega(u^*, v) := \langle \psi | Z_v J Z_u \psi \rangle,$$

and this also defines the matrix Ω as in (26). This matrix is positive semidefinite by

$$(105) \quad \sum_{u,v} \overline{\lambda_u} \lambda_v \omega(u^*, v) = \sum_{u,v} \overline{\lambda_u} \lambda_v \langle \psi | Z_v J Z_u \psi \rangle = \langle \psi | \sum_v \lambda_v Z_v J \sum_u \lambda_u Z_u \psi \rangle \geq 0,$$

where it is essential that J is an anti-unitary operator. Moreover, property (27) is checked by

$$(106) \quad \begin{aligned} \sum_{s,u,t,v} \overline{c_{su}} c_{tv} \Omega_{s^*t, u^*v} &= \sum_{s,u,t,v} \overline{c_{su}} c_{tv} \omega((s^*t)^*, u^*v) \\ &= \sum_{s,u,t,v} \overline{c_{su}} c_{tv} \langle \psi | Z_u^* Z_v J Z_s^* Z_t \psi \rangle = \sum_{s,u,t,v} \overline{c_{su}} c_{tv} \langle Z_u \psi | J J Z_v J Z_s^* Z_t \psi \rangle \\ &= \sum_{s,u,t,v} \overline{c_{su}} c_{tv} \langle Z_u \psi | J Z_s^* Z_t J Z_v \psi \rangle = \sum_{s,u,t,v} \overline{c_{su}} c_{tv} \langle Z_t J Z_v \psi | Z_s J Z_u \psi \rangle \geq 0, \end{aligned}$$

which defines a positive matrix. The linear constrained assertion (31) follows in a similar way. From the previous definitions, we have that

$$(107) \quad \rho_\alpha(D_\beta) = \langle \psi | h_\alpha D_\beta \psi \rangle = \langle \psi | J E_\alpha J D_\beta \psi \rangle = \langle \psi | D_\beta J E_\alpha \psi \rangle = \Omega_{(\alpha), (\beta)},$$

and hence the (infinite-dimensional) matrix Ω fulfills the constraints given by any finite level n as in (32). \square

A.2. Asymptotic Convergence. Here we show that the hierarchy (32)-(33) asymptotically converges to the quantum value (7). The argument follows previous works [19, 41, 36].

Theorem A.2. *Let $\text{sdp}_n[A, \mathcal{F}]$ denote the SDP hierarchy (32)-(33) of the quantum bilinear program (7), including the Archimedian constraints as in (19). Then, we have the following:*

- (1) *In the limit of $n \rightarrow \infty$ the optimal solutions of the programs $\text{sdp}_n[A, \mathcal{F}]$ converge to a finite value,*

$$(108) \quad \lim_{n \rightarrow \infty} \text{sdp}_n[A, \mathcal{F}] = \hat{p}[A, \mathcal{F}].$$

- (2) *There exists a Hilbert space \mathcal{H} , a normalized vector $\xi \in \mathcal{H}$, a $*$ -homomorphism $\pi : \Sigma_\infty \rightarrow \mathcal{B}(\mathcal{H})$ as well as a linear and positive mapping $\varphi : \Sigma_\infty \rightarrow \mathcal{B}(\mathcal{H})$ with commuting ranges (that is, $[\varphi(a), \pi(b)] = 0$ for all $a, b \in \Sigma_\infty$) as well as elements $z_\alpha, y_\beta \in \Sigma_\infty$ such that*

$$(109) \quad \hat{p}[A, \mathcal{F}] = \sum_{\alpha, \beta} A_{\alpha, \beta} \langle \xi | \varphi(z_\alpha) \pi(y_\beta) \xi \rangle.$$

Moreover, the constraints given by the linear functions $g \in \mathcal{G}$ and $k \in \mathcal{K}$ are all satisfied,

$$(110) \quad g(\varphi(z_1), \dots, \varphi(z_N)) \geq 0, \quad \text{as well as} \quad k(\pi(y_1), \dots, \pi(y_M)) \geq 0,$$

in the sense of positive semidefinite operators.

Since the quantum bilinear program (7) is a maximization over all all expressions as on the right-hand side of (109) under the constraints (110), it immediately follows that

$$(111) \quad p^*[A, \mathcal{F}] \geq \hat{p}[A, \mathcal{F}].$$

Now because inequality in the other direction was already established in (95), we conclude that the hierarchy (32)-(33) asymptotically converges to the quantum value (7),

$$(112) \quad p^*[A, \mathcal{F}] = \lim_{n \rightarrow \infty} \text{sdp}_n[A, \mathcal{F}].$$

Furthermore, the optimal value $\bar{p}[A, \mathcal{F}]$ of the algebraic optimization (92) also becomes equal to the quantum value

$$(113) \quad p^*[A, \mathcal{F}] = \bar{p}[A, \mathcal{F}],$$

again by (95).

Proof of Theorem A.2. We first note that due to the Archimedian constraints (19), the positivity constraints provide a bound on the diagonal elements of the $d(1) \times d(1)$ sub-matrix $\Omega_{(\alpha),(\beta)}^n$,

$$(114) \quad C^2 - \Omega_{(\alpha),(\beta)}^n \geq 0,$$

and thus on its trace. Hence, we find that

$$(115) \quad 0 \leq \left| \sum_{\alpha, \beta} A_{\alpha, \beta} \Omega_{(\alpha),(\beta)}^n \right| \leq \|A\| d(1) C^2.$$

Moreover, we have $\text{sdp}_n[A, \mathcal{F}] \leq \text{sdp}_m[A, \mathcal{F}]$ for $n \leq m$. Thus, the sequence $\text{sdp}_n[A, \mathcal{F}]$ is monotonically decreasing and lower bounded by zero, hence converging to a finite value $\hat{p}[A, \mathcal{F}]$.

In order to proceed, we need another expression for the limiting point $\hat{p}[A, \mathcal{F}]$. More precisely, we have to examine in which way the limiting point can be seen as being specified by an infinite-dimensional matrix, capturing the constraints on all words of all possible lengths at once. For any $n \in \mathbb{N}$ we have the subspace $\Sigma_n = \{a \in \Sigma_\infty \mid a = \sum_{w: l(w) \leq n} c_w w\}$. Furthermore, for n odd we define the two families of cones

$$(116) \quad \text{sym}(\Sigma_n) := \left\{ x \in \Sigma_n \otimes \Sigma_n \mid x = \sum_i \lambda_i a_i^* \otimes a_i, \ a_i \in \Sigma_n, \lambda_i \geq 0 \right\}$$

$$(117) \quad (\Sigma_n \otimes \Sigma_n)_+ := \left\{ x \in \Sigma_n \otimes \Sigma_n \mid x = \sum_{\substack{f, \bar{f} \in \mathcal{F} \\ k, l}} a_l^* f a_k \otimes b_k^* \bar{f} b_l, \ a_k, b_k \in \Sigma_{(n-1)/2} \right\}.$$

Let Ω^n be a feasible point of the n -th level of the SDP hierarchy (32). By mapping a pair of words $u, v \in \Sigma_n$ to $\Omega_{u,v}^n$, we specify a linear functional ω on $\Sigma_n \otimes \Sigma_n$, and it is easily seen that the constraints on Ω^n imply that

$$(118) \quad \omega(\text{sym}(\Sigma_n) \cup (\Sigma_n \otimes \Sigma_n)_+) \geq 0, \quad \omega(\mathbb{1}) = 1.$$

For the value

$$(119) \quad p'[A, \mathcal{F}] := \inf \left\{ q : \exists n \text{ with } q\mathbb{1} - \sum_{\alpha, \beta} A_{\alpha, \beta} z_\alpha \otimes y_\beta \in \text{sym}(\Sigma_n) \cup (\Sigma_n \otimes \Sigma_n)_+ \right\},$$

we find that for a finite $\varepsilon > 0$ there exists an $n \in \mathbb{N}$ such that

$$(120) \quad p'[A, \mathcal{F}] + \varepsilon \geq \sum_{\alpha, \beta} A_{\alpha, \beta} \Omega_{(\alpha),(\beta)}^n.$$

Hence, we have $p'[A, \mathcal{F}] \geq \hat{p}[A, \mathcal{F}]$. But by exploiting the Positivstellensatz, a duality argument shows (see, e.g., [19]),

$$(121) \quad p'[A, \mathcal{F}] = \sup \left\{ \left| \sum_{\alpha, \beta} A_{\alpha, \beta} \omega(z_\alpha \otimes y_\beta) \right| : \omega(\text{sym}(\Sigma_\infty) \cup (\Sigma_\infty \otimes \Sigma_\infty)_+) \geq 0, \omega(\mathbb{1}) = 1 \right\},$$

which then implies $p'[A, \mathcal{F}] = \hat{p}[A, \mathcal{F}]$. In the following, we show how to construct a Hilbert space and associated representations, starting from ω .

As usual, the argument is based on a GNS construction, and closely follows the ideas of Woronowicz in his study of purifications for states on C^* -algebras, [54]. We first turn the free algebra Σ_∞ into a C^* -algebra, that is a norm-closed algebra such that we have $\|x^*x\| = \|x\|^2$. This is achieved by defining for $x \in \Sigma_\infty$

$$(122) \quad \|x\| = \sup \{ \|\pi(x)\|_{\mathcal{B}(\mathcal{H}_\pi)} : \pi : \Sigma_\infty \rightarrow \mathcal{B}(\mathcal{H}_\pi) \text{ a }^*\text{-representation} \}.$$

Here, a * -representation is a algebraic homomorphism of Σ_∞ into the bounded operators on some Hilbert space \mathcal{H} such that the * -involution is mapped to the usual involution. It is easily checked

that this norm satisfies our requirement, and thus the topological closure of Σ_∞ under this norm is a C^* -algebra, which we denote by \mathcal{A} . For all $x_i \in \Sigma_\infty$ the Archimedian constraint (19),

$$(123) \quad \exists C : C\mathbb{1} \geq x_i^2,$$

ensures that $\|x_i\| \leq \sqrt{C}$ and hence $x_i \in \mathcal{A}$ since by definition of positivity in \mathcal{A} there exists $w_i \in \mathcal{A}$ with $x_i^*x_i + w_i^*w_i = C\mathbb{1}$ and we have for any $\pi : \mathcal{A} \rightarrow \mathcal{B}(\mathcal{H})$ and any $\psi \in \mathcal{H}, \|\psi\| = 1$

$$(124) \quad \langle \psi | \pi(x_i^2) \psi \rangle \leq \langle \pi(x_i) \psi | \pi(x_i) \rangle + \langle \pi(w_i) \psi | \pi(w_i) \rangle = C.$$

We also define the opposite C^* -algebra $\bar{\mathcal{A}}$, which is as topological space equal to \mathcal{A} equipped with the multiplication rule $a \cdot b = ba$ for $a, b \in \mathcal{A}$. Following [53], we denote a^* as seen as an element of $\bar{\mathcal{A}}$ by \bar{a} . Then the mapping $a \mapsto \bar{a}$ is a $*$ -invariant, anti-linear multiplicative isometry from \mathcal{A} to $\bar{\mathcal{A}}$.

Let $\bar{\mathcal{A}} \otimes \mathcal{A}$ be the maximal C^* -tensor product of $\bar{\mathcal{A}}$ and \mathcal{A} , see for example [42] for a precise definition. On this algebra, we can define another $*$ -invariant, anti-linear and multiplicative mapping $j : \bar{\mathcal{A}} \otimes \mathcal{A} \rightarrow \bar{\mathcal{A}} \otimes \mathcal{A}$ satisfying $j^2 = \text{id}$ by setting

$$(125) \quad j(\bar{a} \otimes b) = \bar{b} \otimes a.$$

We define a state s on $\bar{\mathcal{A}} \otimes \mathcal{A}$ by setting

$$(126) \quad s(\bar{a} \otimes b) = \omega(a^*, b),$$

for words of finite length a, b and then extending to the closure. Normalization is immediate and positivity follows from property $\omega((\Sigma_n \otimes \Sigma_n)_+ \geq 0)$,

$$(127) \quad s((\bar{a} \otimes b)^* \bar{a} \otimes b) = s(\overline{a^*a} \otimes b^*b) = \omega(a^*a, b^*b)$$

since $\bar{x} \cdot \bar{y} = \overline{xy}$.

Carrying out the standard GNS construction for the state s gives rise to a Hilbert space \mathcal{H} , a dense mapping $i : \bar{\mathcal{A}} \otimes \mathcal{A} \rightarrow \mathcal{H}$, a vector $\xi = i(\mathbb{1})$ and a representation $\pi : \bar{\mathcal{A}} \otimes \mathcal{A} \rightarrow \mathcal{B}(\mathcal{H})$ defined by $\pi(\bar{a} \otimes b)i(\bar{c} \otimes d) = i(\overline{ac} \otimes bd)$, such that

$$(128) \quad \langle i(\bar{a} \otimes b) | i(\bar{c} \otimes d) \rangle = \omega(c^*a, b^*d)$$

$$(129) \quad s(\bar{a} \otimes b) = \langle \xi | \pi(\bar{a} \otimes b) \xi \rangle.$$

We now define an anti-linear operator J by defining it on the dense domain $i(\bar{\mathcal{A}} \otimes \mathcal{A})$ as

$$(130) \quad \langle i(\bar{a} \otimes b) | Ji(\bar{c} \otimes d) \rangle = \langle i(\bar{a} \otimes b) | i(\bar{d} \otimes c) \rangle.$$

Its adjoint equals itself, since $\omega(a^*, b) = \overline{\omega(b^*, a)}$ due to positivity and

$$(131) \quad \langle Ji(\bar{a} \otimes b) | i(\bar{c} \otimes d) \rangle = \langle i(\bar{b} \otimes a) | i(\bar{c} \otimes d) \rangle = \omega(c^*b, a^*d) = \overline{\omega(d^*c, b^*a)} = \overline{\langle i(\bar{a} \otimes b) | Ji(\bar{c} \otimes d) \rangle}.$$

Moreover, we find that $J^2 = \mathbb{1}$ and hence J can be extended to an anti-unitary involution on \mathcal{H} . Furthermore, we have

$$(132) \quad J\pi(\bar{a} \otimes b)Ji(\bar{c} \otimes d) = i(\overline{bc} \otimes ad) = \pi(\bar{b} \otimes a)i(\bar{c} \otimes d) = \pi(j(\bar{a} \otimes b))i(\bar{c} \otimes d)$$

and hence $J\pi(\bar{a} \otimes b)J = \pi(j(\bar{a} \otimes b))$. A similar calculation gives

$$(133) \quad \pi(\bar{a} \otimes b) = J\pi(j(\bar{a} \otimes \mathbb{1}))J\pi(\mathbb{1} \otimes b) = \pi(\mathbb{1} \otimes b)J\pi(j(\bar{a} \otimes \mathbb{1}))J.$$

Hence the image of the linear mapping

$$(134) \quad \varphi : a \mapsto \pi(\overline{a^*} \otimes \mathbb{1}) = J\pi(j(\overline{a^*} \otimes \mathbb{1}))J$$

is contained in the commutant of $\pi(\mathbb{1} \otimes \mathcal{A})$. Moreover, any positive element $a^*a \in \mathcal{A}$ gets mapped to

$$(135) \quad \varphi(a^*a) = \pi(\overline{a^*a} \otimes \mathbb{1}) = \pi(\bar{a} \otimes \mathbb{1})^* \pi(\bar{a} \otimes \mathbb{1}),$$

which is a positive operator. This proves (109). The last assertion (110) follows similarly. Considering a linear constraint $k(y_1, \dots, y_M) \in \mathcal{K}$, we find evaluating the diagonal matrix elements of $\pi(\mathbb{1} \otimes k(y_1, \dots, y_M))$ that

$$(136) \quad \langle i(\bar{a} \otimes b) | \pi(\mathbb{1} \otimes k(y_1, \dots, y_M))i(\bar{a} \otimes b) \rangle = \langle i(\bar{a} \otimes b) | i(\bar{a} \otimes k(y_1, \dots, y_M)b) \rangle$$

$$(137) \quad = \omega(a^*a, b^*k(y_1, \dots, y_M)b) \geq 0.$$

Hence $\pi(\mathbb{1} \otimes k(y_1, \dots, y_M))$ is a positive operator. A similar derivation can be carried out for the map φ . \square

APPENDIX B. IMPLICATIONS OF CONNES' EMBEDDING CONJECTURE

In this appendix, we discuss the implications of a positive answer to Connes' embedding conjecture [38, 17] to our hierarchy. We first give a short sketch of an argument why a positive answer to Connes' embedding conjecture implies that the optimization in the program (7) can be restricted to finite-dimensional Hilbert spaces, though it does not imply that this supremum is also achieved. In the second part of this appendix, we sketch the argument for the case of the completely positive-semidefinite cone \mathcal{CS}_+ . As we do not want to go into the details about Connes' embedding conjecture, its different forms and its far reaching consequences (independent of the actual answer), we refer the interested reader to the extensive reviews of Ozawa on the topic [37, 38].

B.1. General case. In Theorem A.2, we found that the limiting point of our SDP hierarchy can be expressed as

$$(138) \quad \hat{p}[A, \mathcal{F}] = \sum_{\alpha, \beta} A_{\alpha, \beta} \langle \xi | \pi^{op}(z_\alpha) \pi(y_\beta) \xi \rangle,$$

where π is a representation of the universal enveloping algebra \mathcal{A} of Σ_∞ , and π^{op} is a representation of the opposite algebra $\bar{\mathcal{A}}$. Let \mathcal{N} be the von Neumann algebra generated by $\pi(\mathcal{A})$. Since we assume that Connes' embedding conjecture holds, all von Neumann algebras satisfy Kirchberg's QWEP property [32] which implies that $\mathcal{N} = \mathcal{B}/\mathcal{J}$, where the C^* -algebra \mathcal{B} has the WEP property, and \mathcal{J} is a two-sided ideal in \mathcal{B} . Since y_β are assumed to be hermitian elements, the Cayley transform U_β of $\pi(y_\beta)$ is a unitary operator. Let $\hat{\pi} : C^*[\mathbb{F}_M] \rightarrow \mathcal{N}$ be the $*$ -homomorphism defined by $s_\alpha \mapsto U_\alpha$, where s_α are the generators of the free group of M elements ($C^*[\mathbb{F}_M]$ is the corresponding universal free group algebra). We apply the same procedure to get another $*$ -homomorphism $\pi^{\hat{op}} : C^*[\mathbb{F}_M]^{op} \rightarrow \pi^{op}(\bar{\mathcal{A}})$. Now, $C^*[\mathbb{F}_M]$ as a free group algebra satisfies the Lifting property [37], and thus the mapping

$$(139) \quad \pi^{\hat{op}} \otimes \hat{\pi} : C^*[\mathbb{F}_M]^{op} \otimes C^*[\mathbb{F}_M] \rightarrow \pi^{op}(\bar{\mathcal{A}}) \pi(\mathcal{A})$$

is continuous with respect to the minimal tensor product, see [32, Proposition 1.3 (iv)]. Correspondingly, the state ω defined by the vector ξ extends to a state $\hat{\omega}$ on the minimal tensor product. As in the proof of [38, Theorem 28], we can assume that the induced representation of $C^*[\mathbb{F}_M]^{op}$ indeed reduces to the opposite representation of $\hat{\pi}(C^*[\mathbb{F}_M])$ on \mathcal{H} . Now we know that $C^*[\mathbb{F}_M]^{op} \otimes C^*[\mathbb{F}_M]$ acts on $S_2(H) = \mathcal{H} \otimes \bar{\mathcal{H}}$ as $(\bar{s} \otimes s)(x) = sx\bar{s}$. Since the state $\hat{\omega}$ can be approximated by a normal state [30], by inverting the Cayley transform we find that for any $\varepsilon > 0$ there exists Hilbert-Schmidt operators $x_i \in S_2(H)$ and hermitian elements $\hat{z}_\alpha, \hat{y}_\beta$ such that

$$(140) \quad \left| \langle \xi | \pi^{op}(z_\alpha) \pi(y_\beta) \xi \rangle - \sum_i \lambda_i \text{Tr} [x_i^* \hat{y}_\beta x_i \hat{z}_\alpha] \right| \leq \varepsilon.$$

But since the state ω originates from an maximization, we can assume that only one term (say given by $x \in S_2(H)$ in the above sum is non-zero. It follows from $\langle \xi | \xi \rangle = 1$ that $\text{Tr}[x^*x] = 1$ and hence we can by an approximation argument assume that x is of finite rank, with support projection p . Projecting the hermitian elements $\hat{z}_\alpha, \hat{y}_\beta$ as well, the form

$$(141) \quad z_\alpha \times y_\beta \rightarrow \text{Tr} [x^* p \hat{y}_\beta p x p \hat{z}_\alpha p]$$

is seen to satisfy all the required constraints. In order to bring it into the form (22), we let $\sigma = |xp|^2$ and find with $x = u|x|$ the polar decomposition of x that $\text{Tr}[\sigma] = \text{Tr}[|x|u^*u|x|] = \text{Tr}[x^*xp] = 1$ as well as

$$(142) \quad \text{Tr} [x^* p \hat{y}_\beta p x p \hat{z}_\alpha p] = \text{Tr} [\sigma^{1/2} \hat{y}_\beta \sigma^{1/2} u \hat{z}_\alpha u^*].$$

B.2. Completely positive semidefinite cone. Theorem A.2 also applies to this case, but we get also from the hierarchy that the constructed state fulfills in addition the cyclicity constraint. More precisely, let s be the state on $\bar{\mathcal{A}} \otimes \mathcal{A}$ constructed in the proof of theorem A.2. Note that in this setting, we do not distinguish two kinds of variables and hence \mathcal{A} is the free C^* -algebra generated by N positive elements z_α , for $\alpha \in \{1, \dots, N\}$. The cyclicity constraints, which are added to each level also hold for the state s , implying that we have

$$(143) \quad s(\overline{z_\alpha \circ u} \otimes v \circ z_\beta) = s(\overline{u \circ z_\beta} \otimes z_\alpha \circ v),$$

where u, v are arbitrary words in the variables z_α . Applying this identity recursively to the choice $z_\beta = \mathbb{I}$, we find for $u = z_{\alpha_1} z_{\alpha_2} \cdots z_{\alpha_n}$

$$(144) \quad s(\bar{u} \otimes v) = s(\overline{z_{\alpha_1} z_{\alpha_2} \cdots z_{\alpha_n}} \otimes v) = s(\overline{z_{\alpha_2} \cdots z_{\alpha_n}} \otimes z_{\alpha_1} \circ v) = \dots = s(\bar{\mathbb{I}} \otimes u^* \circ v).$$

Moreover, by the same trick we find

$$(145) \quad s(\bar{\mathbb{I}} \otimes u \circ z_\alpha) = s(\bar{z}_\alpha \otimes u) = s(\bar{\mathbb{I}} \otimes z_\alpha \circ u),$$

and hence $s(\bar{\mathbb{I}} \otimes u \circ v) = s(\bar{\mathbb{I}} \otimes v \circ u)$. These equalities can be linear extended to hold for all finite polynomials $u, v \in \mathcal{A}$ in the variables z_α , which is a dense subset. They are hence true for all $u, v \in \mathcal{A}$. Since s is a state on $\bar{\mathcal{A}} \otimes \mathcal{A}$, $s(\bar{\mathbb{I}} \otimes \mathcal{A})$ is a state τ on \mathcal{A} , and the constraints just derive imply that it is a tracial state, $\tau(ab) = \tau(ba)$ for $a, b \in \mathcal{A}$. This is also the state which is constructed by the NPA hierarchy, if we would follow the proof steps mentioned in the main text.

It follows from these considerations that the limiting point p^* of our SDP (78) can be written as

$$(146) \quad p^* = \sum_{\alpha, \beta} A_{\alpha, \beta} \tau(z_\alpha z_\beta).$$

Let π_τ be the GNS representation of the state τ , and let $\pi_\tau(\mathcal{A})''$ be the finite von Neumann algebra generated by it. If Connes' embedding conjecture holds, then $\pi_\tau(\mathcal{A})''$ embeds into an ultrapower of the hyperfinite factor, preserving the tracial character of the state. Let θ be this embedding. Then we have

$$(147) \quad p^* = \sum_{\alpha, \beta} A_{\alpha, \beta} \tau \circ \theta^{-1}(\theta(z_\alpha) \theta(z_\beta)),$$

and Burgdorf, Laurent and Piovesan [13] have shown that matrices of the form $\tau \circ \theta^{-1}(\theta(z_\alpha) \theta(z_\beta))$ belong to the closure of the cone \mathcal{CS}_+ .

APPENDIX C. ENTANGLEMENT-ASSISTED NOISY CHANNEL CODING

Here we show that for the channel Z defined in Section 3.2, we have

$$(148) \quad S^*(Z, 1) \geq \frac{1}{2} + \frac{1}{\sqrt{6}} \approx 0.908.$$

For that, we give a quantum protocol using a four dimensional maximally entangled state

$$(149) \quad |\psi\rangle := \frac{1}{2} \sum_{i \in [4]} |i\rangle \otimes |i\rangle.$$

For sending the bit 0, the sender performs a measurement in the computational basis $E(x|0) = |x\rangle\langle x|$ and for sending the bit 1, the sender performs a measurement in the rotated basis $E(x|1) = U|x\rangle\langle x|U^\dagger$ with

$$(150) \quad U = \frac{1}{\sqrt{3}} \begin{pmatrix} 0 & -1 & -1 & 1 \\ 1 & 0 & 1 & 1 \\ -1 & 1 & 0 & 1 \\ -1 & -1 & 1 & 0 \end{pmatrix}.$$

The possible outputs of the channel can be labeled by subsets of the inputs of size 2. We can write the success probability as

$$(151) \quad \frac{1}{6} \sum_{x \in [4], x' \neq x} \langle \psi | |x\rangle\langle x| \otimes D(0|\{x, x'\}) | \psi \rangle + \frac{1}{6} \sum_{x \in [4], x' \neq x} \langle \psi | U|x\rangle\langle x|U^\dagger \otimes (\text{id} - D(0|\{x, x'\})) | \psi \rangle$$

$$(152) \quad = \frac{1}{2} + \frac{1}{6} \sum_{x \in [4], x' \neq x} \langle \psi | (|x\rangle\langle x| - U|x\rangle\langle x|U^\dagger) \otimes D(0|\{x, x'\}) | \psi \rangle$$

$$(153) \quad = \frac{1}{2} + \frac{1}{6} \cdot 2 \sum_{\{x, x'\} \in \binom{[4]}{2}} \langle \psi | \left(\frac{|x\rangle\langle x| + |x'\rangle\langle x'|}{2} - U \frac{|x\rangle\langle x| + |x'\rangle\langle x'|}{2} U^\dagger \right) \otimes D(0|\{x, x'\}) | \psi \rangle.$$

By choosing $D(0|\{x, x'\})$ to be an optimal measurement to distinguish between the states

$$(154) \quad \frac{1}{2}(|x\rangle\langle x| + |x'\rangle\langle x'|) \quad \text{and} \quad \frac{1}{2}U(|x\rangle\langle x| + |x'\rangle\langle x'|)U^\dagger,$$

we get a success probability of

$$(155) \quad \frac{1}{2} + \frac{1}{6} \cdot \frac{1}{4} \sum_{\{x, x'\} \in \binom{[2^n]}{2}} \left\| \frac{|x\rangle\langle x| + |x'\rangle\langle x'|}{2} - U \frac{|x\rangle\langle x| + |x'\rangle\langle x'|}{2} U^\dagger \right\|_1 = \frac{1}{2} + \frac{1}{\sqrt{6}}.$$

APPENDIX D. QUANTUM-PROOF RANDOMNESS EXTRACTORS

Here we give the missing proofs for the claims in Section 3.3. The full first level of our SDP hierarchy (37) for quantum-proof randomness extractors is as follows:

$$(156) \quad \begin{aligned} \text{Err}^{\text{sdP}_1}(\text{Ext}, k) = \underset{\Omega^1}{\text{maximize}} \quad & \frac{1}{2^d} \sum_{i, (s, j)} \left[\delta_{f_s(i)=j} - \frac{1}{2^m} \right] \Omega_{(i), (s, j)}^1 \\ \text{subject to} \quad & \Omega^1 \in \text{Pos}(1 + 2^n + 2^{d+m}) \\ & \Omega_{w, w'}^1 \geq 0 \quad \forall w, w' \in \Sigma_1 \\ & \Omega_{\emptyset, \emptyset}^1 = 1, \quad \Omega_{\emptyset, w}^1 = \sum_i \Omega_{(i), w}^1 \quad \forall w \in \Sigma_1 \\ & 2^{-k} \Omega_{\emptyset, w}^1 \geq \Omega_{(i), w}^1 \quad \forall i \in [2^n], \quad \forall w \in \Sigma_1 \\ & \Omega_{\emptyset, w}^1 \geq \Omega_{(s, j), w}^1 \quad \forall (s, j) \in [2^{d+m}], \quad \forall w \in \Sigma_1 \\ & 2^{-2k} + \Omega_{(i), (i')}^1 \geq 2^{-k} \Omega_{(i), \emptyset}^1 + 2^{-k} \Omega_{\emptyset, (i')}^1 \quad \forall i, i' \in [2^n] \\ & 1 + \Omega_{(s, j), (s', j')}^1 \geq \Omega_{\emptyset, (s', j')}^1 + \Omega_{(s, j), \emptyset}^1 \quad \forall (s, j), (s', j') \in [2^{d+m}] \\ & 2^{-k} + \Omega_{(i), (s, j)}^1 \geq 2^{-k} \Omega_{\emptyset, (s, j)}^1 + \Omega_{(i), \emptyset}^1 \quad \forall i \in [2^n], \quad \forall (s, j) \in [2^{d+m}]. \end{aligned}$$

The upper bound (71) is then immediate by ignoring some constraints.

Proof of Theorem 3.2. The ideas for the proof are from [9, Theorem 5]. We first prove (72). For that we relax the positivity constraint in (71) from

$$(157) \quad \Omega_{(s, j), (s, j)}^1 \geq 0 \quad \text{to} \quad \Omega_{(s, j), (s, j)}^1 \geq -1 \quad \forall (s, j) \in [2^{m+d}],$$

and ignore some of the other constraints in (71) leading to,

$$(158) \quad \begin{aligned} \text{Err}^{\overline{\text{sdP}_1}}(\text{Ext}, k) \leq \underset{\Omega^1}{\text{maximize}} \quad & \frac{1}{2^d} \sum_{i, (s, j)} \left[\delta_{f_s(i)=j} - \frac{1}{2^m} \right] \Omega_{(i), (s, j)}^1 \\ \text{subject to} \quad & \Omega^1 \in \text{Pos}(1 + 2^n + 2^{d+m}) \\ & 0 \leq \Omega_{(i), (i')}^1 \leq 2^{-k} \sum_i \Omega_{(i), (i')}^1 \quad \forall i, i' \in [2^n] \\ & \sum_i \Omega_{(i), (i')}^1 \leq 2^{-k} \quad \forall i' \in [2^n] \\ & \sum_{i, i'} \Omega_{(i), (i')}^1 = 1 \\ & -1 \leq \Omega_{(s, j), (s, j)}^1 \leq 1 \quad \forall (s, j) \in [2^{m+d}]. \end{aligned}$$

Moreover, we write $\Omega^1 \in \text{Pos}(1 + 2^n + 2^{d+m})$ as a Gram matrix:

$$(159) \quad \Omega_{u, u'}^1 =: \vec{a}_u \cdot \vec{a}_{u'}, \quad \Omega_{u, v}^1 =: \vec{a}_u \cdot \vec{b}_v, \quad \Omega_{v, v'}^1 =: \vec{b}_v \cdot \vec{b}_{v'} \quad \forall u, u' \in [2^n] \cup \{\emptyset\}, \quad \forall v, v' \in [2^{m+d}] \cup \{\emptyset\}.$$

An application of the Cauchy-Schwarz inequality then easily reveals that the optimal choice for $\vec{b}_{(s, j)}$ is

$$(160) \quad \vec{b}_{(s, j)} = \frac{\sum_i [\delta_{f_s(i)=j} - \frac{1}{2^m}] \vec{a}_i}{\left\| \sum_i [\delta_{f_s(i)=j} - \frac{1}{2^m}] \vec{a}_i \right\|_2}.$$

Thus, the upper bound program becomes

$$\begin{aligned}
 \text{Err}^{\overline{\text{sdp}_1}}(\text{Ext}, k) &\leq \underset{\vec{a}_i}{\text{maximize}} \quad \frac{1}{2^d} \sum_{(s,j)} \left\| \sum_i \left[\delta_{f_s(i)=j} - \frac{1}{2^m} \right] \vec{a}_i \right\|_2 \\
 &\text{subject to} \quad 0 \leq \vec{a}_i \cdot \vec{a}_{i'} \leq 2^{-k} \sum_i \vec{a}_i \cdot \vec{a}_{i'} \quad \forall i, i' \in [2^n] \\
 &\quad \sum_i \vec{a}_i \cdot \vec{a}_{i'} \leq 2^{-k} \quad \forall i' \in [2^n] \\
 &\quad \sum_{i, i'} \vec{a}_i \cdot \vec{a}_{i'} = 1.
 \end{aligned}
 \tag{161}$$

Again using the Cauchy-Schwarz inequality we can write

$$\frac{1}{2^d} \sum_{(s,j)} \left\| \sum_i \left[\delta_{f_s(i)=j} - \frac{1}{2^m} \right] \vec{a}_i \right\|_2 \leq \sqrt{\frac{1}{2^d} \sum_{(s,j)} \left\| \sum_i \left[\delta_{f_s(i)=j} - \frac{1}{2^m} \right] \vec{a}_i \right\|_2^2} \sqrt{2^m}.
 \tag{162}$$

Letting (again),

$$\Omega_{(i),(i')}^1 = \vec{a}_i \cdot \vec{a}_{i'} \quad \text{and} \quad \bar{\Omega}_{(i)}^1 := \sum_{i'} \Omega_{(i),(i')}^1,
 \tag{163}$$

we look at the expression

$$\frac{1}{2^d} \sum_{(s,j)} \left\| \sum_i \left[\delta_{f_s(i)=j} - \frac{1}{2^m} \right] \vec{a}_i \right\|_2^2 = \frac{1}{2^d} \sum_{(s,j)} \sum_{i, i'} \left[\delta_{f_s(i)=j} - \frac{1}{2^m} \right] \cdot \left[\delta_{f_s(i')=j} - \frac{1}{2^m} \right] \Omega_{(i),(i')}^1
 \tag{164}$$

$$\leq \frac{1}{2^d} \sum_{(s,j)} \sum_i \bar{\Omega}_{(i)}^1 \left| \sum_{i'} \left[\delta_{f_s(i')=j} - \frac{1}{2^m} \right] \frac{\Omega_{(i),(i')}^1}{\bar{\Omega}_{(i)}^1} \right|
 \tag{165}$$

$$\leq \frac{1}{2^d} \sum_{(s,j)} \left| \sum_i \delta_{f_s(i)=j} 2^{-k} - \frac{1}{2^m} \right|,
 \tag{166}$$

where we made use of the constraints in (161) for the last inequality. Going back to the error $\text{Err}(\text{Ext}, k)$ as in (64) we conclude the claim.

We now prove (73). We upper bound $\text{Err}^{\overline{\text{sdp}_1}}(\text{Ext}, k)$ by forgetting several constraints and then apply Grothendieck's inequality (see Lemma D.1 below):

$$\text{Err}^{\overline{\text{sdp}_1}}(\text{Ext}, k) \leq \max \left\{ \frac{1}{2^d} \sum_{i, (s,j)} \left(\delta_{f_s(i)=j} - \frac{1}{2^m} \right) \vec{a}_i \cdot \vec{b}_{(s,j)} : \|\vec{a}_i\|_2 \leq 2^{-k}, \|\vec{b}_{(s,j)}\|_2 \leq 1 \right\}
 \tag{167}$$

$$\leq K_G \max \left\{ \frac{1}{2^d} \sum_{i, (s,j)} \left(\delta_{f_s(i)=j} - \frac{1}{2^m} \right) a_i b_{(s,j)} : |a_i| \leq 2^{-k}, |b_{(s,j)}| \leq 1 \right\}
 \tag{168}$$

$$\leq K_G \max \left\{ \frac{1}{2^d} \sum_{(s,j)} \left| \sum_i \left(\delta_{f_s(i)=j} - \frac{1}{2^m} \right) a_i \right| : |a_i| \leq 2^{-k} \right\}.
 \tag{169}$$

We partition the set of $i \in [2^n]$ into $\{i : a_i \geq 0\}$ and $\{i : a_i < 0\}$, and write

$$\left| \sum_i \left(\delta_{f_s(i)=j} - \frac{1}{2^m} \right) a_i \right| \leq \left| \sum_{i: a_i \geq 0} \left(\delta_{f_s(i)=j} - \frac{1}{2^m} \right) a_i \right| + \left| \sum_{i: a_i < 0} \left(\delta_{f_s(i)=j} - \frac{1}{2^m} \right) (-a_i) \right|.
 \tag{170}$$

Let us write

$$\alpha_+ := \sum_{i: a_i \geq 0} a_i.
 \tag{171}$$

Now if $\alpha_+ \geq 1$, then we define

$$(172) \quad p_+(i) := \frac{\max\{a_i, 0\}}{\alpha_+}.$$

Observing that $\alpha_+ \leq 2^{n-k}$, we have

$$(173) \quad \frac{1}{2^d} \sum_{(s,j)} \left| \sum_{i: a_i \geq 0} \left(\delta_{f_s(i)=j} - \frac{1}{2^m} \right) a_i \right| = \alpha_+ \cdot \frac{1}{2^d} \sum_{(s,j)} \left| \sum_i \left(\delta_{f_s(i)=j} - \frac{1}{2^m} \right) p_+(i) \right|$$

$$(174) \quad \leq 2\alpha_+ \text{Err}(\text{Ext}, k + \log(\alpha_+))$$

$$(175) \quad \leq 2 \cdot 2^{n-k} \text{Err}(\text{Ext}, k),$$

with the error $\text{Err}(\text{Ext}, k)$ as in (64). Otherwise, if $\alpha_+ < 1$, then we define

$$(176) \quad p_+(i) := \max\{a_i, 0\} + (1 - \alpha_+)2^{-n}.$$

We have

$$(177) \quad \begin{aligned} & \frac{1}{2^d} \sum_{(s,j)} \left| \sum_{i: a_i \geq 0} \left(\delta_{f_s(i)=j} - \frac{1}{2^m} \right) a_i \right| \\ &= \frac{1}{2^d} \sum_{(s,j)} \left| \sum_i \left(\delta_{f_s(i)=j} - \frac{1}{2^m} \right) (p_+(i) - (1 - \alpha_+)2^{-n}) \right| \end{aligned}$$

$$(178) \quad \leq \frac{1}{2^d} \sum_{(s,j)} \left| \sum_i \left(\delta_{f_s(i)=j} - \frac{1}{2^m} \right) p_+(i) \right| + (1 - \alpha_+) \frac{1}{2^d} \sum_{(s,j)} \left| \sum_i \left(\delta_{f_s(i)=j} - \frac{1}{2^m} \right) 2^{-n} \right|$$

$$(179) \quad \leq 2\text{Err}(\text{Ext}, k - 1) + 2(1 - \alpha_+)\text{Err}(\text{Ext}, n).$$

With a similar argument for the set $\{i : a_i < 0\}$, we reach the bound

$$(180) \quad \begin{aligned} & \frac{1}{2^d} \sum_{(s,j)} \left| \sum_i \left(\delta_{f_s(i)=j} - \frac{1}{2^m} \right) a_i \right| \\ & \leq 2 \max \left\{ 2 \cdot 2^{n-k} \text{Err}(\text{Ext}, k), \text{Err}(\text{Ext}, k - 1) + \text{Err}(\text{Ext}, n) + 2^{n-k} \text{Err}(\text{Ext}, k), \right. \end{aligned}$$

$$(181) \quad \left. 2\text{Err}(\text{Ext}, k - 1) + (1 - \alpha_+ - \alpha_-)\text{Err}(\text{Ext}, n) \right\}$$

$$(182) \quad \leq 6 \cdot 2^{n-k} \text{Err}(\text{Ext}, k - 1).$$

From this we conclude the claim

$$(183) \quad \text{Err}^{\overline{\text{sdp}_1}}(\text{Ext}, k) \leq 6 \cdot 2^{n-k} \text{Err}(\text{Ext}, k - 1).$$

□

Lemma D.1 (Grothendieck's inequality). *For any real matrix $\{A_{ij}\}$, we have*

$$(184) \quad \max \left\{ \sum_{i,j} A_{ij} \vec{a}_i \cdot \vec{b}_j : \|\vec{a}_i\|_2 \leq 1, \|\vec{b}_j\|_2 \leq 1 \right\} \leq K_G \cdot \max \left\{ \sum_{i,j} A_{ij} a_i b_j : a_i, b_j \in \mathbb{R}, |a_i| \leq 1, |b_j| \leq 1 \right\}.$$

ACKNOWLEDGMENTS

We thank Hamza Fawzi and Thomas Vidick for helpful discussions. We would also like to thank Allhussein Fawzi and Hamza Fawzi for their help with writing and running MATLAB code. Part of this work was done while VBS was visiting the École Normale Supérieure de Lyon and part of it while visiting the Institute for Quantum Information and Matter at Caltech, we thank John Preskill and Thomas Vidick for their hospitality. VBS acknowledges partial support by the EU project Randomness and Quantum Entanglement (RAQUEL) and the NCCR QSIT.

REFERENCES

- [1] L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational complexity*, 1(1):3–40, 1991.
- [2] S. Barman and O. Fawzi. Algorithmic aspects of optimal channel coding. 2015. Available online: <http://arxiv.org/abs/1508.04095>.
- [3] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3):195–200, 1964.
- [4] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. Multi-prover interactive proofs: how to remove intractability assumptions. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 113–131. ACM, 1988.
- [5] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Physical Review Letters*, 76(5):722, 1996.
- [6] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal. Entanglement-assisted classical capacity of noisy quantum channels. *Physical Review Letters*, 83(15):3081, 1999.
- [7] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69(20):2881, 1992.
- [8] M. Berta, O. Fawzi, and V. B. Scholz. Quantum-proof randomness extractors via operator space theory. 2014. Available online: <http://arxiv.org/abs/1409.3563>.
- [9] M. Berta, O. Fawzi, and V. B. Scholz. Semidefinite programs for randomness extractors. In *TQC’15: Proceedings of the 10th conference on Theory of quantum computation, communication, and cryptography*. Springer-Verlag, 2015. Available online: <http://perso.ens-lyon.fr/omar.fawzi/pubs/extractors-sdp.pdf>.
- [10] M. Berta, F. Furrer, and V. B. Scholz. The smooth entropy formalism on von Neumann algebras. 2011. Available online: <http://arxiv.org/abs/1107.5460>.
- [11] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86(2):419–478, 2014.
- [12] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf. Nonlocality and communication complexity. *Reviews of Modern Physics*, 82(1):665–698, 2010.
- [13] S. Burgdorf, M. Laurent, and T. Piovesan. On the closure of the completely positive semidefinite cone and linear approximations to quantum colorings. 2015. Available online: <http://arxiv.org/abs/1502.02842>.
- [14] P. J. Cameron, A. Montanaro, M. W. Newman, S. Severini, and A. Winter. On the quantum chromatic number of a graph. *Electronic Journal of Combinatorics*, 14(1), 2007.
- [15] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880, 1969.
- [16] R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Computational Complexity, 2004. Proceedings. 19th IEEE Annual Conference on*, pages 236–249. IEEE, 2004.
- [17] A. Connes. Classification of injective factors. Cases II_1 , II_∞ , III_λ , $\lambda \neq 1$. *Annals of Mathematics. Second Series*, 104:73–115, 1976.
- [18] T. S. Cubitt, D. Leung, W. Matthews, and A. Winter. Improving zero-error classical communication with entanglement. *Physical Review Letters*, 104(23):230503, 2010.
- [19] A. C. Doherty, Y.-C. Liang, B. Toner, and S. Wehner. The Quantum Moment Problem and Bounds on Entangled Multi-prover Games. In *2008 23rd Annual IEEE Conference on Computational Complexity*, pages 199–210. IEEE, 2008.
- [20] P. Fermé. Randomness extractors: Complexity and relaxations. Technical report, Department of Computing and Mathematical Sciences, Caltech, 2015.
- [21] P. E. Frenkel and M. Weiner. On vector configurations that can be realized in the cone of positive matrices. *Linear Algebra and its Applications*, 459:465 – 474, 2014.
- [22] T. Fritz. Tsirelson’s problem and Kirchberg’s conjecture. *Reviews in Mathematical Physics*, 24(05):1250012, 2012.
- [23] T. Fritz, T. Netzer, and A. Thom. Can you compute the operator norm? *Proceedings of the American Mathematical Society*, 142(12):4265–4276, 2014.
- [24] M. Grant and S. Boyd. Graph implementations for nonsmooth convex programs. In V. Blondel, S. Boyd, and H. Kimura, editors, *Recent Advances in Learning and Control*, Lecture Notes in Control and Information Sciences, pages 95–110. Springer-Verlag Limited, 2008.
- [25] M. Grant and S. Boyd. CVX: Matlab software for disciplined convex programming, version 2.1. <http://cvxr.com/cvx>, 2014.
- [26] R. Haag. *Local Quantum Physics: Fields, Particles, Algebras*. Springer, 1992.
- [27] B. Hemenway, C. A. Miller, Y. Shi, and M. Wootters. Optimal entanglement-assisted one-shot classical communication. *Physical Review A*, 87(6):062301, 2013.
- [28] M. Junge, M. Navascués, C. Palazuelos, D. Perez-Garcia, V. B. Scholz, and R. F. Werner. Connes’ embedding problem and Tsirelson’s problem. *Journal of Mathematical Physics*, 52:012102, 2011.
- [29] M. Junge and C. Palazuelos. Large violation of Bell inequalities with low entanglement. *Communications in Mathematical Physics*, 306:695–746, 2011.
- [30] R. Kadison and J. Ringrose. *Fundamentals of the Theory of Operator Algebras: Elementary theory*. Fundamentals of the Theory of Operator Algebras. American Mathematical Society, 1997.
- [31] J. Kempe, O. Regev, and B. Toner. Unique games with entangled provers are easy. *SIAM Journal on Computing*, 39(7):3207–3229, 2010.

- [32] E. Kirchberg. On non-semisplit extensions, tensor products and exactness of group C^* -algebras. *Inventiones mathematicae*, 112:449–489, 1993.
- [33] J.-B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM Journal on Optimization*, 11(3):796–817, 2001.
- [34] M. Laurent and T. Piovesan. Conic approach to quantum graph parameters using linear optimization over the completely positive semidefinite cone. 2013. Available online: <http://arxiv.org/abs/1312.6643>.
- [35] M. Navascués, S. Pironio, and A. Acín. Bounding the set of quantum correlations. *Physical Review Letters*, 98:010401, 2007.
- [36] M. Navascués, S. Pironio, and A. Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, 2008.
- [37] N. Ozawa. About the QWEP conjecture. *International Journal of Mathematics*, 15(05):501–530, 2004.
- [38] N. Ozawa. About the Connes embedding conjecture: algebraic approaches. *Japanese Journal of Mathematics*, 8:147–183, 2013.
- [39] K. F. Pál and T. Vértesi. Quantum bounds on Bell inequalities. *Physical Review A*, 79(2):022120, 2009.
- [40] P. A. Parrilo. Semidefinite programming relaxations for semialgebraic problems. *Mathematical Programming*, 96(2):293–320, 2003.
- [41] S. Pironio, M. Navascués, and A. Acín. Convergent Relaxations of Polynomial Optimization Problems with Non-commuting Variables. *Siam Journal on Optimization*, 20(5):2157–2180, Jan. 2010.
- [42] G. Pisier. *Introduction to operator space theory*, volume 294. Cambridge University Press, 2003.
- [43] R. Prevedel, Y. Lu, W. Matthews, R. Kaltenbaek, and K. J. Resch. Entanglement-enhanced classical communication over a noisy classical channel. *Physical Review Letters*, 106(11):110505, 2011.
- [44] R. Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich, 2005.
- [45] D. Roberson and L. Mancinska. Graph homomorphisms for quantum players. 2012. Available online: <http://arxiv.org/abs/1212.1724>.
- [46] V. B. Scholz and R. F. Werner. Tsirelson’s problem. 2008. Available online: <http://arxiv.org/abs/0812.4305>.
- [47] J. Sikora and A. Varvitsiotis. Linear conic formulations for two-party correlations and values of nonlocal games. 2015. Available online: <http://arxiv.org/abs/1506.07297>.
- [48] M. Takesaki. *Theory of Operator Algebras I*. Springer, 2001.
- [49] M. Takesaki. *Theory of Operator Algebras II*. Springer, 2002.
- [50] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover hashing against quantum side information. *Information Theory, IEEE Transactions on*, 57:5524–5535, 2011.
- [51] S. P. Vadhan. Pseudorandomness. *Foundations and Trends in Theoretical Computer Science*, 7(1–3):1–336, 2011.
- [52] H. T. Williams and P. Bourdon. Entanglement enhancement of a noisy classical communication channel. 2011. Available online: <http://arxiv.org/abs/1109.1029>.
- [53] S. Woronowicz. On the purification of factor states. *Communications in Mathematical Physics*, 28(3):221–235, 1972.
- [54] S. Woronowicz. On the purification map. *Communications in Mathematical Physics*, 30(1):55–67, 1973.

INSTITUTE FOR QUANTUM INFORMATION AND MATTER, CALTECH, PASADENA, CA 91125, USA
E-mail address: `berta@caltech.edu`

DEPARTMENT OF COMPUTING AND MATHEMATICAL SCIENCES, CALTECH, PASADENA, CA 91125, USA
 LIP¹⁰, ÉCOLE NORMALE SUPÉRIEURE DE LYON, LYON, 69007, FRANCE
E-mail address: `omar.fawzi@ens-lyon.fr`

INSTITUTE FOR THEORETICAL PHYSICS, ETH ZÜRICH, 8093 ZÜRICH, SWITZERLAND
E-mail address: `scholz@phys.ethz.ch`

¹⁰UMR 5668 LIP - ENS Lyon - CNRS - UCBL - INRIA, Université de Lyon